ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник наукових праць V Міжнародної науково-практичної конференції ІБІТ 2024

27 листопада 2024 року

Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет “Львівська політехніка”

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІБІТ 2024

Збірник наукових праць
V Міжнародної науково-практичної конференції

27 листопада 2024 року

Львів – 2024

ББК 32.81+78.362
І 74

Інформаційна безпека та інформаційні технології: збірник наукових праць V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, Растр-7, 2024, 636 с.

ISBN 978-617-8537-86-9

ISBN 978-617-8537-86-9

ЧЛЕНИ ПРОГРАМНОГО КОМІТЕТУ:

Ростислав Львович ТКАЧУК – доктор технічних наук, професор, начальник кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності.

Олександр Володимирович ПРИДАТКО – кандидат технічних наук, доцент, проректор з навчальної та методичної роботи Львівського державного університету безпеки життєдіяльності.

Богдан Васильович ДУРНЯК – доктор технічних наук, професор, в.о. ректора Української академії друкарства.

Любомир Степанович СІКОРА – доктор технічних наук, професор, професор кафедри автоматизованих систем управління Національного університету "Львівська політехніка".

Валерій Богданович ДУДИКЕВИЧ – доктор технічних наук, професор, професор кафедри захисту інформації Національного університету "Львівська політехніка".

Іван Романович ОПІРСЬКИЙ – доктор технічних наук, професор, завідувач кафедри захисту інформації Національний університет "Львівська політехніка".

Ігор Михайлович ЖУРАВЕЛЬ – доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного університету "Львівська політехніка".

Максим Володимирович КОРОБЧИНСЬКИЙ – доктор технічних наук, професор п'ятої кафедри Воєнно-дипломатичної академія ім. Євгенія Березняка Міністерства оборони України.

Роман Святославович ЯКОВЧУК – доктор технічних наук, доцент, начальник факультету цивільного захисту, Львівський державний університет безпеки життєдіяльності.

Володимир Афанасійович РОМАКА – доктор технічних наук, професор, профе-

сор кафедри захисту інформації Національного університету “Львівська політехніка”.

Volodymyr SAMOTYY – prof. dr hab. inż., professor, Katedra Automatyki i Informatyki Politechnika Krakowska im. Tadeusza Kościuszki.

Sergii TELENYK – prof. dr hab. inż., professor, Department of automatic control and computer engineering Cracow University of Technology.

Наталя Корнеліївна ЛИСА – доктор технічних наук, професор, доцент кафедри автоматизованих систем управління Національного університету “Львівська політехніка”.

Тарас Євгенович РАК – доктор технічних наук, доцент, професор кафедри інформаційних технологій ПЗВО “ІТ СТЕП Університет”.

Zbigniew KOKOSIŃSKI – dr hab. Inż., prof. PK kierownik Katedry Politechnika Krakowska im. Tadeusza Kościuszki.

Тетяна Олександрівна ГОВОРУЩЕНКО – доктор технічних наук, професор, декан факультету інформаційних технологій Хмельницького національного університету

Ольга Володимирівна МЕНЬШИКОВА – кандидат фізико-математичних наук, доцент, заступник начальника факультету цивільного захисту, Львівський державний університет безпеки життєдіяльності.

Назарій Євгенович БУРАК – кандидат технічних наук, доцент, заступник начальника кафедри інформаційних технологій та систем електронних комунікацій, Львівський державний університет безпеки життєдіяльності.

Sofiia KUTAS team lead of security and access management department in NBS, United Kingdom and Ireland.

Amiran SHARADZE – PhD student, Assistant of the Department of computer sciences, Batumi Shota Rustaveli State University.

РЕДКОЛЕГІЯ:

Ростислав ТКАЧУК – д.т.н., професор, начальник кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності.

Олександр ПРИДАТКО – к.т.н., доцент, проректор з навчальної та методичної роботи Львівського державного університету безпеки життєдіяльності.

Іван ОПІРСЬКИЙ – д.т.н., професор, професор, завідувач кафедри захисту інформації Національного університету “Львівська політехніка”.

Валерій ДУДИКЕВИЧ – д.т.н., професор, професор кафедри захисту інформації Національного університету “Львівська політехніка”.

Zbigniew KOKOSIŃSKI – dr hab. Inż., prof. PK kierownik Katedry Politechnika Krakowska im. Tadeusza Kościuszki.

Volodymyr SAMOTYY – prof. dr hab. inż., professor, Katedra Automatyki i Informatyki Politechnika Krakowska im. Tadeusza Kościuszki.

Sergii TELENYK – prof. dr hab. inż., professor, Department of automatic control and computer engineering Cracow University of Technology.

Володимир РОМАКА – д.т.н., професор, професор кафедри захисту інформації Національного університету “Львівська політехніка”.

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

Секція 1

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

Напрям 1

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ВІЙНИ

УДК 004.056

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ТА NFT ДЛЯ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ДЕРЖАВНИХ РЕЄСТРІВ

Валерія БАЛАЦЬКА*[1]*,
***Василь ПОБЕРЕЖНИК*[2]**

[1]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

[2]Кафедра захисту інформації Національного Університету "Львівська Політехніка", м. Львів, Україна.

Abstract. *The explores the potential of blockchain and NFT technologies to manage access control to public registries in Ukraine. It reviews the principles of blockchain as a decentralized database and NFTs as unique digital identifiers that enable precise access control, enhancing data security and transparency in public registry management.*

Keywords: *blockchain, NFT, data access, public registries, confidentiality, identification.*

Анотація. *Досліджено можливості застосування технологій блокчейн та NFT для забезпечення розмежування доступу до державних реєстрів України. Розглянуто принципи роботи блокчейн як децентралізованої бази даних та NFT як унікальних цифрових ідентифікаторів, що дозволяють контролювати доступ до інформації, підвищуючи безпеку та прозорість управління даними.*

Ключові слова: *блокчейн, NFT, доступ до даних, державні реєстри, конфіденційність, ідентифікація.*

Використання цифрових технологій стало невід'ємною частиною сучасного управління даними, особливо у сфері державних реєстрів. Із зростанням викликів, пов'язаних із конфіденційністю, захистом та доступністю інформації, впровадження інноваційних рішень є життєво необхідним. Застосування блокчейн та NFT є перспективним підходом для розмежування доступу до державних реєстрів, що вже демонструє свою ефективність у різних сферах, від фінансових операцій до управління правами власності.

Блокчейн – це децентралізована база даних, що забезпечує збереження записів транзакцій у незмінному вигляді. Кожен блок зв'язується з попереднім через хеш, утворюючи ланцюг, що забезпечує цілісність і неможливість змін без узгодження всієї мережі [1]. Така структура робить блокчейн ідеальним для застосування в системах, де необхідні надійні записи, які неможливо підробити. NFT (Non-Fungible Tokens), у свою чергу, є унікальними цифровими активами, що дозволяють точно визначати права доступу до ресурсів і створювати механізми управління власністю [2].

Однак централізовані системи управління державними реєстрами залишаються вразливими до корупції, підробок та кіберзлочинності, що може поставити під загрозу конфіденційність і цілісність інформації [3]. Використання блокчейн та NFT допомагає мінімізувати ці ризики завдяки децентралізованій природі зберігання даних і механізмам цифрової ідентифікації [4]. *Наприклад*, усі транзакції в блокчейн фіксуються у хронологічному порядку і доступні для перевірки, що підвищує довіру до системи.

З огляду на ці характеристики, блокчейн забезпечує високу стійкість до несанкціонованих змін, прозорість і можливість аудиту. Це дозволяє ефективно відстежувати операції та запобігати фальсифікаціям [5]. Використання смарт-контрактів забезпечує автоматизацію процесів управління доступом, дозволяючи надавати його за певних умов, таких як верифікація користувача чи виконання інших критеріїв безпеки [6]. Смарт-контракти є важливим інструментом, що додає гнучкості й автоматизації в системи управління доступом.

Застосування NFT для ідентифікації та контролю доступу є особливо ефективним. Кожен токен містить унікальний цифровий підпис, що підтверджує його автентичність і унеможливлює підробку [7]. Використання NFT для розмежування доступу до даних дозволяє чітко визначати, хто має право на доступ до конкретних даних, і сприяє підвищенню прозорості та безпеки управління інформацією.

Це особливо важливо для державних реєстрів, де доступ до певної інформації має бути обмеженим на рівні користувачів. Завдяки унікальним цифровим токенам можна розмежувати права доступу до даних, забезпечуючи контроль над тим, хто може переглядати чи змінювати інформацію. Такий підхід дозволяє підвищити ефективність системи, роблячи її більш надійною та захищеною.

Технологічні компоненти системи включають блокчейн-платформу для збереження даних та NFT для управління правами доступу. Використання криптографічних ключів забезпечує автентифікацію: приватний ключ використовується для підпису транзакцій, а публічний – для перевірки підпису.

Це створює надійне середовище для безпечного управління даними, де кожна операція є захищеною та прозорою.

Впровадження блокчейн та NFT у державні реєстри супроводжується певними викликами. Серед них висока вартість реалізації, необхідність інтеграції з наявними системами та регуляторні питання. *Наприклад*, питання захисту приватних ключів користувачів є критичним, адже їх втрата може призвести до недоступності даних. Для подолання цих проблем потрібні нові стандарти та політики, що регулюють використання блокчейн та NFT. Також необхідно підвищувати рівень обізнаності персоналу, проводити навчання та залучати експертів з кібербезпеки для впровадження цих технологій.

Висновки. Загалом, застосування блокчейн та NFT для управління доступом до державних реєстрів може значно підвищити безпеку, прозорість та ефективність управління інформацією. Попри певні виклики, ці технології мають потенціал стати основою для побудови сучасної цифрової інфраструктури, забезпечуючи захист даних та зміцнення довіри громадян до державних органів.

Інформаційні джерела

1. Балацька В. С., Опірський І. Р., Побережник В. О. Використання Non-Fungible Tokens та блокчейн для розмежування доступу до державних реєстрів // Кібербезпека: освіта, наука, техніка. – 2024. – № 4 (24). – С. 99–114. URL: https://doi.org/10.28925/2663-4023.2024.24.99114.

2. Опірський І., Балацька В., Побережник В. Сучасні можливості використання блокчейн-технології в освітній системі // Ukrainian Scientific Journal of Information Security. – 2023. – Vol. 29, Issue 3. – С. 138–146. URL: https://doi.org/10.18372/2225-5036.29.18073.

3. Побережник В., Балацька В., Опірський І. Розробка концепції системи управління навчанням на основі блокчейн-технології // CEUR Workshop Proceedings. – 2023. – Vol. 3550.

4. Balatska V., Opirskyy I., Slobodian N., Blockchain for enhancing transparency and trust in government registries, CPITS-II 2024: Cybersecurity Providing in Information and Telecommunication Systems II. – 2024, pp. 50–59.

5. Poberezhnyk V., Balatska V., Opirskyy I., Development of the Learning Management System Concept based on Blockchain Technology, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 143–156.

6. Dong M., Wang X., Niyato D., & Han Z. Blockchain for Secure and Trustworthy IoT: A Survey // IEEE Access. – 2021. – Vol. 9, pp. 4955–4971. URL: https://doi.org/10.1109/JIOT.2019.2920987.

7. Singh P., & Singh K. A review on security and privacy issues in blockchain technology // Materials Today: Proceedings. – 2021. – Vol. 44, pp. 3495–3498. URL: https://doi.org/0.1201/9781003022688-11.

УДК 004.42:65.012.1

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В СУЧАСНИХ РЕАЛІЯХ

Наталія ФЕДИНЕЦЬ,
Олександр СИНИЦЯ
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *Every year, the number and complexity of cyberattacks increases, which requires enterprises to implement effective protection systems. The volume of processed information, including personal data of customers, is increasing. Inadequate protection can lead to financial losses and loss of customer trust. Many countries introduce strict norms and standards in the field of information security (GDPR, ISO/IEC 27001, etc.), which obliges enterprises to comply with certain standards. A security breach can cause serious reputational damage. Thus, effective management of information security is critically important for the sustainable development of enterprises and their competitiveness in the modern world.*

Keywords: *information security, security, management, cyber attacks, network security, monitoring tools.*

Анотація. *З кожним роком зростає кількість і складність кібератак, що вимагає від підприємств запровадження ефективних систем захисту. Зростає обсяг оброблюваної інформації, включаючи персональні дані клієнтів. Неналежний захист може призвести до фінансових втрат і втрати довіри з боку клієнтів. Багато країн вводять жорсткі норми і стандарти в сфері інформаційної безпеки (GDPR, ISO/IEC 27001 тощо), що зобов'язує підприємства дотримуватись певних стандартів. Інформаційна безпека стає важливою складовою іміджу компанії. Порушення безпеки може завдати серйозної шкоди репутації. Таким чином, ефективний менеджмент інформаційної безпеки є критично важливим для сталого розвитку підприємств і їхньої конкурентоспроможності в сучасному світі.*

Ключові слова: *інформаційна безпека, безпека, менеджмент, кібератаки, безпека мережі, інструменти моніторингу.*

З розвитком нових технологій, таких як штучний інтелект і блокчейн, виникають нові можливості для покращення інформаційної безпеки. Менеджмент інформаційної безпеки – це процес, що включає в себе планування, реалізацію, контроль та удосконалення заходів, спрямованих на захист інформації від несанкціонованого доступу, знищення, зміни або пошкоджен-

ня. Це комплексний підхід, який охоплює технологічні, організаційні та людські аспекти забезпечення інформаційної безпеки.

Основні компоненти менеджменту інформаційної безпеки включають:

Оцінку ризиків. Виявлення та оцінка потенційних загроз та вразливостей інформаційних активів. Це дозволяє зрозуміти, які ризики є найбільш критичними для організації.

Політику та процедури. Розробка документів, що визначають правила і процедури для забезпечення інформаційної безпеки. Політики повинні бути зрозумілими та доступними для всіх співробітників.

Технічні заходи. Впровадження засобів захисту, таких як антивірусне програмне забезпечення, системи виявлення вторгнень, шифрування даних та брандмауери.

Навчання та обізнаність. Проведення регулярних навчань для співробітників з питань інформаційної безпеки, щоб підвищити їх обізнаність про загрози та найкращі практики.

Моніторинг та аудит. Постійний контроль за виконанням політик і процедур, а також періодичні аудити для виявлення недоліків та можливостей для покращення.

Відновлення після інцидентів. Розробка планів на випадок інцидентів, що дозволяють швидко відновити нормальну діяльність організації після можливих атак чи витоків інформації.

Менеджмент інформаційної безпеки в умовах воєнного стану має ряд особливостей, які зумовлені специфічними викликами та загрозами:

1. Зростання ризиків і загроз:

– кібернетичні атаки (під час воєнного конфлікту зростає ймовірність кібернетичних атак з боку ворога. Це може включати в себе хакерські атаки, фішинг, віруси тощо;

– фізична загроза (інфраструктура, в тому числі інформаційні системи, може бути під загрозою фізичних атак або руйнувань).

2. Швидкість реагування:

– адаптивність (необхідність швидкої адаптації стратегій і тактик інформаційної безпеки у відповідь на змінювані обставини та загрози);

– план дій на випадок надзвичайних ситуацій (розробка та впровадження планів дій для швидкого реагування на інциденти);

3. Забезпечення безпеки комунікацій:

– захист інформації (посилення заходів для захисту каналів комунікації, оскільки інформація може бути перехоплена або спотворена);

– шифрування (використання шифрування для захисту чутливої інформації).

4. Навчання та обізнаність:

– регулярне навчання: Підвищення обізнаності співробітників щодо нових загроз та методів захисту.

– тренінги з кризового управління (проведення навчань, що фокусуються на реагуванні на інциденти в умовах війни).

5. Складність управління ресурсами:

– обмеженість ресурсів (можливе зменшення фінансування та ресурсів для забезпечення інформаційної безпеки);

– робота з віддаленими командами (під час воєнного стану можуть бути обмеження на пересування, тому важливо забезпечити безпеку віддалених робочих місць).

6. Співпраця з державними органами:

– взаємодія з правоохоронними органами (тісна співпраця з державними структурами для обміну інформацією про загрози та інциденти);

– участь у національних програмах безпеки (залучення до національних ініціатив і програм з інформаційної безпеки).

7. Фокус на критично важливі системи:

– пріоритетність (визначення критично важливих інформаційних систем та ресурсів, які потребують особливого захисту в умовах війни).

8. Оцінка та аудит

– регулярний моніторинг (постійний моніторинг стану інформаційної безпеки та аудит вразливостей для своєчасного виявлення загроз).

Висновки. Загалом, слід зазначити, що менеджмент інформаційної безпеки в умовах воєнного стану вимагає системного, адаптивного підходу, а також тісної взаємодії між усіма зацікавленими сторонами для забезпечення максимальної захищеності інформаційних активів.

Інформаційні джерела

1. Бакуліч О. О. Інформаційна безпека як важлива складова функціонування бізнесу в умовах військового стану. Варіативні моделі й технології трансформації професійного розвитку фахівців в умовах відкритої освіти: зб. матер. Всеукр. наук.-практ. інтернет-конф., 23 червня 2022 р. [ред. кол.: Пуховська Л. П., Просіна О. В. та ін.]. – К. : ДЗВО “Ун-т менеджменту освіти”, 2022. – 461 с.

2. Пугачевська Й. К., Мартин А. В. Інформаційна безпека в умовах воєнного стану. Управління соціально-економічними трансформаціями господарських процесів: реалії і виклики: збірник тез доповідей V Міжнародної науково-практичної конференції. – Мукачево: МДУ, 2023. – 195 с.

УДК 004.056

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ПОТОКІВ БАНКІВСЬКОЇ УСТАНОВИ

Орест ПОЛОТАЙ

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The information flows of banking institutions that require protection are described. The main stages of the life cycle of the project for implementing a system for protecting information flows of a banking institution are studied. The main works for implementing a project for protecting banking information are considered.*

Keywords: *information security, banking institution.*

Анотація. *Описано інформаційні потоки банківських установ, які потребують захисту. Досліджено основні етапи життєвого циклу проекту запровадження системи захисту інформаційних потоків банківської установи. Розглянуто основні роботи запровадження проекту захисту банківської інформації.*

Ключові слова: *інформаційна безпека, банківська установа*.

Як відомо, сучасна банківська установа – це універсальна установа, що прагне здійснювати якомога більше видів операцій, які спрямовані на забезпечення її функціонування, з одного боку, як суб'єкта підприємницької діяльності, з іншого – як фінансового посередника, який здійснює властиві йому функції. Якщо розглядати банківську установу, як проектну організацію, то основними її цілями є якісне надання послуг своїм клієнтам (замовникам, споживачам продукту проекту) при умові забезпечення свого існування та функціонування.

В сучасних умовах, коли широкого розповсюдження набуло використання обчислювальної техніки і засобів обміну інформацією, виникають канали її можливого просочення та несанкціонованого доступу до неї зі сторони зловмисників. Особливо вразливими сьогодні залишаються обчислювальні мережі та серверне програмне забезпечення. Інформація, циркулююча в них, може бути незаконно змінена, викрадена або знищена [5].

Враховуючи вищесказане, для забезпечення виконання поставлених перед банківською установою цілей, необхідно дотримуватися ряд вимог, правил та процедур інформаційної безпеки. Інформаційна безпека виступає сучасним процесом, який є необхідним для забезпечення безпеки інформаційних ресурсів будь-яких організацій, зокрема і банківських установ, що в свою чергу є однією з умов досягнення їх проектних цілей. Для виконання вимог, що висуваються правилами інформаційної безпеки є дотримання вимог захисту об'єктів інформаційної діяльності, які цього потребують. Осно-

вними об'єктами захисту банківської установи виступають її інформаційні потоки. Тому виникає необхідність запроваджувати систему захисту інформаційних потоків банківської установи.

Під інформаційним потоком банківської установи розуміють сукупність даних, які циркулюють в її межах та необхідні для здійснення управлінських процесів. Проходження інформаційних потоків у банківській установі забезпечують сучасні інформаційні системи та технології. Необхідність проекту запровадження системи захисту інформаційних потоків банківської установи спрямований на підтримку ефективної роботи згаданих інформаційних систем та технологій. Основними нормативними документами, що визначають основні напрями та способи реалізації проектів в сфері захисту банківських установ, зокрема їх інформаційних потоків, є закон України "Про інформацію" та ряд інших законів, постанов, правил та стандартів.

Необхідність у запровадженні такого проекту фактично задекларована у стандартах 27001, 27002 виданих Національним Банком України.

Оскільки основним призначенням проекту виступає захист інформаційних потоків, то варто визначитись, які саме інформаційні потоки необхідно захищати. Іншими словами, яку сферу інформаційної діяльності банківської установи повинен захищати продукт проекту, а саме система захисту.

Отже, основні інформаційні потоки банківської установи, які потребують захисту, можна розділити на наступні групи:

– інформаційні потоки в центральній автоматизованій системі "Операційний день банку";

– інформаційні потоки в внутрішньобанківській міжфілійній платіжній системі;

– інформаційні потоки в міжбанківських платіжних системах в Національній та іноземній валютах;

– інформаційні потоки в платіжних системах банківських автоматів обслуговування пластикових платіжних карт;

– інформаційні потоки в телекомунікаційній системі віддаленого управління рахунками клієнтів "Клієнт-Банк", "Інтернет-Банкінг";

– інформаційні потоки в системах "електронної пошти".

Варто зазначити, що продуктом проекту запровадження системи захисту інформаційних потоків банківської установи є створена комплексна система захисту інформаційних потоків, під якою розуміють взаємопов'язану сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації від розголошення, витоку і несанкціонованого доступу [4].

Життєвий цикл проекту системи захисту інформаційних потоків банківської установи включає ряд етапів [6]:

– формування вимог до системи захисту інформаційних потоків банківської установи;

– розроблення політики безпеки;

– розроблення технічного завдання на створення системи захисту інформаційних потоків банківської установи;

– створення проекту системи захисту інформаційних потоків банківської установи;

– введення в дію системи захисту;

– супровід системи захисту.

Одними із складових наведених вище етапів, без яких не може бути реалізований будь-який проект, що пов'язаний із запровадженням системи захисту інформації, є множина робіт Р, що представлена у вигляді кортежу:

$$P = \{ПП, ООЗ, ТКВІ, МП, МЗ, ТПЗ, ОЗ\},$$

де, *ПП* – детальний план приміщення, в якому існують об'єкти, що потребують захисту (інформаційні потоки) та буде функціонувати продукт проекту;

ООЗ – опис об'єктів захисту, заради яких потрібно запроваджувати проект, в даному випадку під об'єктами захисту розуміється автоматизована система банківської установи;

ТКВІ – опис можливих технічних каналів витоку інформації;

МП – опис моделі порушника конфіденційності, цілісності та доступності інформаційних об'єктів захисту;

МЗ – опис моделі можливих загроз інформаційних потоків;

ТПЗ – пропозиції по введенню в дію технічних та програмних засобів захисту інформаційних потоків, з метою заблокування *ТКВІ*;

ОЗ – розроблення політики організаційного захисту інформаційних потоків банківської установи.

Важливим елементом представленого кортежу виступають технічні канали витоку інформації *(ТКВІ)*, оскільки саме через них відбувається можливий витік інформаційних потоків за потенційні межі зони дії продукту проекту – контрольованої зони. Розглянемо основні *ТКВІ*, що притаманні автоматизованій системі банківської установи (табл. 1).

Таблиця 1.

Технічні канали витоку інформації через основні складові автоматизованої системи

Визначення та перелік об'єктів які підлягають захисту		*Можливий витік за рахунок*
Основні складові автоматизованої системи	Персональні комп'ютери	випромінювання електромагнітних сигналів, які потім можуть перехоплюватись випадковими антенами, перегляду сторонніми особами зображення на моніторі, спостереження сторонніми особами за роботою з клавіатурою, несанкціонованого доступу до оперативної пам'яті чи накопичувачів комп'ютера.

	Локальна мережа з виходом у Internet	проникнення в неї вірусів і закладок, перегляду; сторонніми особами зображення на моніторі, спостереження сторонніми особами за роботою з клавіатурою, несанкціонованого доступу до оперативної пам'яті чи накопичувачів комп'ютера.
	Копіювально-розмножувальна техніка	випромінювання електромагнітних сигналів, спостереження сторонніми особами за їх роботою, дії на них сторонніх осіб.
	Сигнальні лінії мережі Ethernet	наведення на технічні засоби, інші проводи та кабелі, які розміщені на відстанях, менш критичних.

Безпека банку визначається як стан стійкої життєдіяльності, при якому забезпечується реалізація основних інтересів і пріоритетних цілей банку, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов функціонування.

Висновки. Отже у процесі розроблення концепції управління банківською діяльністю варто виділити основні процеси функціонування банківської установи і виключити можливість витоку інформації, її несанкціонованого використання, нанесення збитків, упущення вигоди з боку всіх зацікавлених сторін і в напрямі досягнення основних цілей банківської діяльності. Реалізація цих положень гармонійно вписується в концепцію корпоративного управління банківською діяльністю, до якої сьогодні залучаються дедалі більше банківських установ. Управління інформаційною безпекою банківської установи і повинно стати частиною цієї концепції.

Інформаційні джерела

1. Ахрамович В. М. Курс лекцій з навчальної дисципліни "Кібербезпека банківських та комерційних структур" / В. М. Ахрамович. Державний університет телекомунікацій. – К.: ДУТ, 2019. – 163 с.

2. Закон України "Про інформацію" від 2 жовтня 1992 року N 2658-XII // Із змінами і доповненнями, внесеними Законами України станом від 23 червня 2005 року N 2707-IV.

3. Закон України "Про банки та банківську діяльність" [Закон України „Про банки і банківську діяльність" від 7 грудня 2000 року N 2121-III // Із змінами і доповненнями, внесеними Законами України станом від 12 грудня 2008 року N 661-VI.

4. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 № 80/94-ВР Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). URL: https://ela.kpi.ua/server/api/core/bitstreams/e5c73b24-058a-42d8-bd2d-03a17e2c7c9a/content.

5. Козаченко І. П., Голубєв В. О. Загальні принципи захисту інформації в банківських автоматизованих системах. URL://www.bezpeka.com/ru/lib/spec/infsys/art92.html.

6. НД ТЗІ 3.7-003-2005. Про порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

УДК 004.49

ВІРУСИ-ДРОППЕРИ: ТЕХНІКИ ДОСТАВКИ ШКІДЛИВОГО ПЗ ТА ОБХІД ЗАХИСНИХ СИСТЕМ

Артур ТКАЧЕНКО
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *This work outlines the unique characteristics of dropper viruses and their behaviors within operating systems.*
Keywords: *dropper, behavioral analysis.*

Анотація. *Описано особливості вірусів-дропперів та їх поведінку в операційних ситемах.*
Ключові слова: *дроппер, поведінковий аналіз.*

Віруси-дроппери є одними з найпоширеніших інструментів для поширення шкідливого програмного забезпечення (ШПЗ), забезпечуючи успішну доставку та встановлення небажаних компонентів на пристрій жертви. Дроппери можуть приховувати свою активність за рахунок багатоступеневих процесів та обфускації коду, що ускладнює їх виявлення. Їхнє використання особливо небезпечне через широкий спектр шкідливих дій, які можуть виконуватися на інфікованих системах, включно з крадіжкою даних, контролем системи або зараженням мереж.

Головне завдання дроппера – приховано доставити основне ШПЗ або інші шкідливі компоненти на цільову систему. На першому етапі дроппер встановлює файл з основною загрозою. Часто дроппер містить вбудовані алгоритми, що обходять антивірусний захист, такі як шифрування або маскування поведінки, що ускладнює їх виявлення на ранніх стадіях зараження.

Сучасні дроппери поділяються на два основні типи: одноступеневі (single-stage) та багатоступеневі (multi-stage). Одноступеневі дроппери негайно розгортають основну загрозу після потрапляння в систему. Багатоступеневі дроппери, навпаки, використовують кілька етапів для поступового розгортання шкідливих компонентів, що дозволяє їм уникати антивірусного контролю, який може не відразу визначити загрозу через приховані дії. Багатоступеневі дроппери особливо небезпечні, оскільки на кожному етапі можуть додавати нові компоненти або навіть встановлювати інші дроппери для багаторазової доставки шкідливого ПЗ на ту ж систему.

Виявлення дропперів вимагає складних методів аналізу, таких як поведінковий аналіз, оскільки статичні методи не завжди спрацьовують через їхню здатність до маскування. *Наприклад*, поведінковий аналіз дозволяє виявити підозрілі дії програм у системі, такі як аномальні записи у файлову систему, нестандартні мережеві запити або неконтрольований запуск проце-

сів. Деякі антивірусні системи використовують технології штучного інтелекту для розпізнавання прихованих шкідливих шаблонів, хоча дроппери постійно адаптуються та вдосконалюють обхід захисних бар'єрів.

Для ефективної протидії дропперам рекомендується поєднувати кілька засобів захисту. Це включає оновлення операційних систем та ПЗ, щоб уникнути вразливостей, використання багаторівневих антивірусних рішень з поведінковим аналізом, а також налаштування політик мережевої безпеки, які обмежують небезпечні дії та контроль над сторонніми програмами. Обмеження доступу до небезпечних сайтів та використання фаєрволів для моніторингу мережевих активностей також можуть значно знизити ризик зараження через дроппери.

Висновки. Дроппери представляють складну та адаптивну загрозу для сучасних ІТ-систем. Оскільки їхня здатність уникати традиційного виявлення постійно вдосконалюється, інтеграція сучасних засобів захисту з поведінковим аналізом є ключем до запобігання інфікування. Швидке виявлення шкідливих дій на ранніх етапах та підвищена кіберобізнаність є найкращим захистом від цих складних загроз.

Інформаційні джерела

1. Full analysis dropper malware 0x01 – MalGamy. URL: https://malgamy.github.io/malware-analysis/Analysis-dropper-malware/

2. Zillya! Dropper F. URL: https://zillya.ua/virus/dropper_f

3. Understanding Dropper Malware: Types, Examples, Detection, and Prevention – Perception Point. URL: https://perception-point.io/guides/malware/understanding-dropper-malware-types-examples-detection-and-prevention/

УДК 351.74

СУЧАСНІ ВИКЛИКИ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ В УМОВАХ ВІЙНИ

Валентина ЯЩУК
Богдан ОШУРКО
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The theoretical, scientific-methodical and organizational-functional foundations of state secret protection in wartime conditions are considered. Modern approaches to state secret protection in modern realities are identified. Methodological approaches to forming the concept of a state secret protection system are presented. Stages of solving the scientific-practical problem associated with increasing the level of state secret protection are proposed.*

Keywords: *protection of state secrets, cybersecurity, information warfare, critical infrastructure, disinformation, international cooperation.*

Анотація. *Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи захисту державної таємниці в умовах війни. Визначено сучасні підходи до захисту державної таємниці у сучасних реаліях. Наведено методичні підходи до формування концепції системи захисту державної таємниці. Запропоновано етапи вирішення науково-практичної проблеми, пов'язаної з підвищенням рівня захисту державної таємниці.*

Ключові слова: *захист державної таємниці, кібербезпека, інформаційна війна, критична інфраструктура, дезінформація, міжнародне співробітництво.*

Захист державної таємниці в умовах війни сьогодні набуває особливої актуальності в контексті сучасних геополітичних реалій, що характеризуються посиленням міжнародної напруженості та зростанням кіберзагроз. Сучасні війни все частіше набувають гібридного характеру, де інформаційна війна є невід'ємною складовою. Кібератаки, дезінформація, маніпуляції громадською думкою – все це стає потужним інструментом впливу на суспільство та державу. У таких умовах захист державної таємниці набуває стратегічного значення для забезпечення національної безпеки. Швидкий розвиток інформаційних технологій, штучного інтелекту, великих даних створює нові можливості як для захисту інформації, так і для її викрадення. Зловмисники використовують ці технології для створення більш складних і витончених атак, що ускладнює завдання захисту державної таємниці.

Сучасні держави все більше залежать від критичної інфраструктури (енергетика, транспорт, комунікації), яка є вразливою до кібератак. Компрометація такої інфраструктури може мати катастрофічні наслідки для економіки та безпеки держави. В умовах війни зростає ризик витоку інформації через ненавмисні дії персоналу, шантаж, вербування та інші внутрішні загрози. Існуюча нормативно-правова база в багатьох країнах не завжди встигає за розвитком технологій та новими видами загроз. Це створює додаткові труднощі у забезпеченні захисту державної таємниці.

Дослідження захисту державної таємниці в умовах війни дозволить систематизувати та узагальнити сучасні виклики в захисті державної таємниці в умовах війни шляхом розроблення нових підходів та рекомендації щодо підвищення фективності захисту державної таємниці та проведення аналізу існуючих нормативно-правових актів та виявлення прогалини, що потребують усунення.

Сучасні війни все частіше мають гібридний характер, де інформаційна війна є одним із ключових інструментів боротьби. Тому, підвищення ефективності захисту державної таємниці є одним із пріоритетних завдань для забезпечення національної безпеки будь-якої держави. Інтеграція всіх державних органів та критичної інфраструктури в єдину систему кіберзахисту дозволить ефективніше протидіяти кіберзагрозам. Поряд з цим використання штучного інтелекту, машинного навчання та інших сучасних технологій для виявлення та нейтралізації кіберзагроз та проведення навчань та тренінгів для персоналу з метою підвищення обізнаності про кіберзагрози та фор-

мування навичок безпечної роботи в мережі сприятиме підвищенню ефективності захисту державної таємниці в умовах війни.

Проведення імітаційних атак для визначення оцінки стійкості критичної інфраструктури до кіберзагроз, створення резервних копій критично важливих даних та їх зберігання в безпечному місці, розроблення детальних планів дій на випадок кібератак та інших надзвичайних ситуацій забезпечує захист критичної інфраструктури. Забезпечення додаткового рівня захисту шляхом використання двофакторної аутентифікації при доступі до секретної інформації, моніторинг переліку осіб, які більше не потребують доступу до секретної інформації, вдосконалення системи доступу та допуску до державної таємниці, та засобів фізичного захисту для зберігання носіїв інформації, що містять державну таємницю вдосконалить систему доступу до державної таємниці.

Сьогодні виникає гостра потреба у формуванні у суспільства критичного мислення та здатності відрізняти правдиву інформацію від фейків, що забезпечує об'єктивне висвітлення подій та протидіє поширенню фейкових новин шляхом створення спеціалізованих структур для виявлення, аналізу та нейтралізації дезінформації. Розширення міжнародного співробітництва в галузі кібербезпеки, обмін досвідом, технологіями та розвідданими з партнерами для спільного протистояння кіберзагрозам а також участь у діяльності міжнародних організацій, що займаються питаннями кібербезпеки сприятиме підвищенню ефективності захисту державної таємниці в умовах війни.

Організація багаторівневої системи охорони державної таємниці в умовах воєнного стану є невід'ємною складовою забезпечення національної безпеки України. Вона є ефективним інструментом запобігання розголошенню критично важливої інформації, знижує ризик несанкціонованого доступу та сприяє захисту державних інтересів. Багаторівневий підхід, який поєднує комплекс заходів фізичної та інформаційної безпеки, сучасні технології ідентифікації, шифрування, а також регулярний контроль за дотриманням процедур доступу, дозволяє забезпечити високий рівень конфіденційності в умовах постійних загроз. Результати дослідження можуть бути використані для розроблення нових стратегій та тактик захисту державної таємниці. З метою вдосконалення нормативно-правової бази в сфері захисту державної таємниці шляхом розроблення навчальних програм для фахівців у галузі інформаційної безпеки.

Запровадження системного підходу до захисту державної інформації є важливим чинником підтримки стабільності державного управління та координації дій у сфері оборони та безпеки. Крім того, в умовах підвищеної вразливості до інформаційних та кіберзагроз критично важливою є адаптація існуючих процедур до динамічних викликів війни, що вимагає постійного моніторингу та вдосконалення охоронних механізмів.

Висновки. Захист державної таємниці в умовах війни є складним і багатогранним завданням, яке вимагає комплексного підходу. Реалізація запропонованих заходів дозволить значно підвищити рівень захищеності державної таємниці та забезпечити національну безпеку.

Інформаційні джерела

1. Ящук В. І. Принципи проектування автоматизованих інформаційних систем управління об'єктами критичної інфраструктури.Сучасні напрями розвитку економіки, підприємництва, технологій та їх правового забезпечення: матеріали Міжнародної науково-практичної конференції / [відповід. за вип. : проф. Семак Б. Б.]. – Львів : вид-во Львівського торговельно-економічного університету, 2021. – 328 с. С. 292–294.

2. Ящук В., Ткачук Р., Івануса А. Оцінювання ризиків кібербезпеки об'єктів критичної інфраструктурию. Інформаційна безпека та інформаційні технології: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – Львів: Растр-7, 2022. – 380 с. С. 67–70.

УДК 004.93:351.74

ОЦІНЮВАННЯ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА СИСТЕМУ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ

Валентина ЯЩУК
Вікторія СТОЛЯРЧУК
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The theoretical, scientific-methodical and organizational-functional foundations of the impact of artificial intelligence on the state secret protection system are considered. Modern approaches to the protection of state secrets in modern realities are identified. Methodological approaches to the formation of the concept of assessing the impact of artificial intelligence on the state secret protection system are presented. Stages of solving the scientific and practical problem of the impact of artificial intelligence on the state secret protection system are proposed.*

Keywords: *state secret protection, artificial intelligence, cybersecurity, information warfare, critical infrastructure, disinformation.*

Анотація. *Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи впливу штучного інтелекту на систему захист державної таємниці. Визначено сучасні підходи до захисту державної таємниці у сучасних реаліях. Наведено методичні підходи до формування концепції оцінювання впливу штучного інтелекту на систему захисту державної таємниці. Запропоновано етапи вирішення науково-практичної проблеми впливу штучного інтелекту на систему захисту державної таємниці.*

Ключові слова: *захист державної таємниці, штучний інтелект, кібербезпека, інформаційна війна, критична інфраструктура, дезінформація.*

Штучний інтелект (ШІ) стрімко розвивається і все більше проникає в усі сфери людської діяльності, в тому числі і в сферу безпеки. Застосування ШІ в захисті державної таємниці має як значні переваги, так і потенційні ризики. Тому, оцінка впливу ШІ на захист державної таємниці є надзвичайно актуальною науковою проблемою.

Існуючі дослідження в цій галузі в основному зосереджені на аналізі потенційних загроз, які можуть виникнути внаслідок використання ШІ, зокрема, ризик зловмисного використання ШІ, проблема розмежування відповідальності, ризик упередженості алгоритмів. ШІ може бути використаний для створення більш складних і ефективних кібератак, розробки нових видів зброї та дезінформації. Хто несе відповідальність за дії систем, що базуються на ШІ, якщо вони призведуть до витоку державної таємниці. Алгоритми ШІ можуть містити в собі упередження, що може призвести до прийняття неправильних рішень.

Разом з тим, існують дослідження, які розглядають позитивні аспекти використання ШІ в захисті державної таємниці, такі як: автоматизація рутинних завдань, покращення точності аналізу даних, створення більш ефективних систем захисту. ШІ може автоматизувати багато рутинних завдань, пов'язаних з аналізом великих обсягів даних, що дозволяє звільнити фахівців для виконання більш складних задач. ШІ здатний виявляти загрози, які можуть бути пропущені людським аналітиком. ШІ може бути використаний для розробки більш інтелектуальних систем захисту інформації, які здатні адаптуватися до нових загроз.

Разом з тим невирішеними залишаються питання забезпечення безпечного використання ШІ в державних органах, правові та етичні проблеми при використанні ШІ в захисті державної таємниці, оцінювання ризиків, пов'язаних з використанням ШІ, та розроблення ефективних заходів протидії, забезпечення прозорості систем, що базуються на ШІ.

Вплив ШІ на захист державної таємниці спричиняє виникнення як загроз так і можливостей. Серед основних загроз можна виокремити створення кібератак більшої складності, генерація дезінформації, соціальна інженерія. ШІ може бути використаний для автоматизації процесу пошуку вразливостей в системах безпеки, розробки нових видів шкідливого програмного забезпечення та проведення масштабних DDoS-атак. Також ШІ може бути використаний для створення великих обсягів фейкових новин та інших видів дезінформації, що може дестабілізувати суспільство і підірвати довіру до державних інституцій. ШІ може бути використаний для створення більш переконливих фішингових листів та інших видів соціальної інженерії, що дозволяє здобувати конфіденційну інформацію.

Досліджуючи можливості варто відзначити збільшення ефективності аналізу даних, автоматизація рутинних завдань, розроблення нових методів захисту. ШІ може аналізувати великі обсяги даних в режимі реального часу,

виявляючи підозрілу активність та прогнозуючи потенційні загрози. ШІ може автоматизувати багато рутинних завдань, таких як моніторинг мережі, аналіз логів та ідентифікація загроз, що дозволяє звільнити фахівців для виконання більш складних задач. ШІ може бути використаний для розроблення нових методів захисту інформації, таких як адаптивні системи захисту, які здатні самонавчатися і адаптуватися до нових загроз.

Штучний інтелект є потужним інструментом, який може бути використаний як для захисту, так і для атаки. Для того щоб максимізувати переваги ШІ і мінімізувати ризики, виникає потреба у розробленні комплексного підходу до його використання в сфері безпеки. Цей підхід повинен включати в себе розроблення ефективних систем управління ризиками, створення правової бази, міжнародне співробітництво, постійне навчання та підвищення кваліфікації фахівців. Запровадження комплексного підходу вимагає розроблення методів оцінювання ризиків, пов'язаних з використанням ШІ, та розроблення заходів для їх мінімізації. Також виникає потреба у розробленні нових правових норм, які регулюють використання ШІ в сфері безпеки. Співпраця з іншими країнами для розробки спільних стандартів безпеки ШІ дозволить підвищити ефективність захисту таємної інформації.

Загалом, ШІ відкриває нові можливості для забезпечення безпеки держави, але його використання потребує обережного та зваженого підходу. Підсумовуючи викладене вище, можна виокремити такі рекомендації, як розвиток національних стратегій в галузі кібербезпеки, які враховуватимуть використання ШІ, інвестування в дослідження та розробки в галузі ШІ та кібербезпеки, створення міжнародних форумів для обговорення питань, пов'язаних з використанням ШІ в сфері безпеки, розроблення системи сертифікації систем ШІ, що використовуються в державних органах, проводити навчання та підвищення кваліфікації фахівців в галузі ШІ та кібербезпеки.

Незважаючи на значну кількість досліджень в цій галузі, багато питань залишаються відкритими. Необхідно проводити подальші дослідження в таких напрямках, як розроблення методів оцінювання стійкості систем ШІ до атак, дослідження впливу ШІ на міжнародну безпеку та розробка нових алгоритмів машинного навчання для виявлення аномалій в мережевому трафіку. Завдяки впровадженню цих рекомендацій можна мінімізувати ризики, пов'язані з використанням ШІ, та максимізувати його потенціал для забезпечення національної безпеки. Використання ШІ в захисті державної таємниці є перспективним напрямком досліджень, який вимагає подальшого розвитку.

Інформаційні джерела

1. Ящук В. І. Роль та місце стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави. Moderní aspekty vědy: XLII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. p. 364. pp. 259–286.

2. Ящук В. І. Методика забезпечення безпеки інформаційних систем та реагування на кіберінциденти кібербезпековими центрами. Scientific Collection “InterConf+”, 45(201): with the Proceedings of the 8thInternational Scientific and Practical Conference “International Scientific Discussion: Problems, Tasks and Prospects” (May19–20, 2024; Brighton, United Kingdom)/ comp. by LLC SPC “InterConf”.Brighton: A.C.M. Webb Publishing Co Ltd., 2024. 678 p. pp. 632–641.

УДК 004.056.5

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ВОЄННИЙ ЧАС

Вадим ВИГЛАЗОВ
Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам’янець-Подільський, Україна.

Abstract. *The article addresses the protection of personal data under martial law, focusing on practical measures to ensure confidentiality. Special attention is paid to data security in cloud services and on mobile devices. Recommendations include device protection, access management, encryption, and data backup. The author emphasizes the importance of combining legal frameworks with personal responsibility to safeguard data in the digital environment.*
Keywords: *personal data protection, martial law, cloud services, mobile devices, confidentiality, encryption, data backup, national security.*

Анотація. *У доповіді розглядаються аспекти захисту персональних даних в умовах воєнного стану, зокрема практичні заходи для забезпечення їх конфіденційності. Окрема увага приділяється безпеці даних у хмарних сервісах та на мобільних пристроях. Рекомендації включають захист пристроїв, управління доступом, використання шифрування та створення резервних копій. Автор наголошує на необхідності поєднання правових норм та особистої відповідальності для захисту даних у цифровому середовищі.*
Ключові слова: *захист персональних даних, воєнний стан, хмарні сервіси, мобільні пристрої, конфіденційність, шифрування, резервне копіювання, національна безпека.*

Вступ. В умовах воєнного стану в Україні питання захисту персональних даних стало ще більш актуальним. З одного боку, держава має право встановлювати певні обмеження в цій сфері для забезпечення національної безпеки. З іншого боку, громадяни мають право захищати особисті дані від незаконного збору, використання та розповсюдження.

Виклад основного матеріалу. Як ми знаємо, захист персональних даних в умовах воєнного стану залишається пріоритетом. Хоча GDPR та інші закони Про захист даних мають певні обмеження, вони все ще забезпечують базовий

рівень захисту персональних даних. Але крім правових норм, є й інші практичні кроки, які ви можете зробити, щоб максимально захистити себе:

1. Ретельно діліться своїми даними:

– Обмежте кількість інформації, яку Ви публікуєте в Інтернеті, особливо в соціальних мережах.

– Не передавайте свої особисті дані незнайомим людям або невідомим веб-сайтам.

– Використовуйте надійні паролі для всіх своїх облікових записів в інтернеті та регулярно змінюйте їх.

2. Захист пристрою:

– Встановіть надійне антивірусне програмне забезпечення та програмне забезпечення для захисту даних на свій комп'ютер або мобільний пристрій.

– Регулярно оновлюйте операційну систему та програмне забезпечення.

– Використовуйте VPN під час підключення до загальнодоступної мережі Wi-Fi.

3. Будь ласка, будьте пильні:

– Остерігайтеся фішингових листів і веб-сайтів, які намагаються вимагати ваші особисті дані.

– Не відкривайте підозрілі посилання або жовтні вкладення.

– Слідкуйте за іноземними дзвінками, які запитують Вашу особисту інформацію.

4. Знайте свої права:

– Ознайомтеся з GDPR та іншими законами Про захист даних, щоб зрозуміти ваші права та обмеження.

– Якщо ви підозрюєте, що ваші особисті дані були оброблені незаконно, зверніться до компетентних державних органів [1].

Конфіденційність даних у хмарі: Зберігання даних у хмарі стає все більш поширеним способом доступу до інформації з будь-якого місця та з будь-якого пристрою. Однак, зберігаючи особисті або конфіденційні дані в хмарі, важливо знати про ризики та вживати заходів для їх мінімізації.

Ось кілька важливих моментів, які слід знати про конфіденційність хмарних даних:

1. Вибір постачальника хмарних послуг:

– Віддайте перевагу надійним та надійним постачальникам послуг з чіткою репутацією безпеки даних.

– Будь ласка, ознайомтеся з Політикою конфіденційності та умовами використання постачальника, щоб зрозуміти, як Ваші дані використовуються і захищені.

– Переконайтеся, що ваш провайдер використовує новітні технології безпеки, такі як шифрування даних і контроль доступу.

2. Захист даних:

– Доступ до хмарного сховища з використанням надійних паролів і двофакторної аутентифікації.

– Не діліться своїм паролем з іншими.

– Шифруйте конфіденційні дані перед їх зберіганням у хмарі.

– Регулярно оновлюйте програмне забезпечення вашого пристрою.

3. *Контроль доступу*:

– Надайте доступ до своїх даних лише тим, хто їх дійсно потребує.

– Використовуйте списки контролю доступу, щоб обмежити, хто може переглядати, редагувати або видаляти дані.

– Моніторинг активності в хмарному сховищі і виявлення підозрілої активності.

4. Резервне копіювання та відновлення:

– Створюйте регулярні резервні копії своїх даних, щоб ви могли відновити їх у разі збою або втрати.

– Зберігайте резервну копію окремо від основних даних у безпечному місці.

– Перевірте план відновлення вашого хмарного провайдера, щоб дізнатися, що робити в разі аварії.

Будь ласка, пам'ятайте:

– Конфіденційність даних у хмарі-це спільна відповідальність.

– Виберіть надійного постачальника,

– Вживайте запобіжних заходів для захисту ваших даних,

– Контролюйте доступ до них,

– Регулярно створюйте резервні копії.

– Дотримуючись цих порад, ви можете зберегти свої дані приватними та безпечними у хмарі [2].

Захист даних на мобільних пристроях: захистить свою кишеню в цифровому світі. У сучасному світі мобільні пристрої стали невід'ємною частиною нашого життя. Ми використовуємо їх для спілкування, роботи, розваг і зберігання важливої інформації. Однак при зберіганні особистих або конфіденційних даних на мобільних пристроях важливо вживати заходів для захисту від несанкціонованого доступу, втрати або пошкодження. Ось кілька важливих порад про те, як захистити свої дані на мобільному пристрої:

1. *Захист пристрою*:

– Встановіть захищений PIN-код, пароль або шаблон для блокування екрана.

– Використовуйте біометричні функції, такі як розпізнавання відбитків пальців та обличчя, Якщо ваш пристрій підтримує їх.

– Увімкніть віддалене блокування та видалення даних, щоб ви могли заблокувати або стерти дані зі свого пристрою у разі його втрати або крадіжки.

– Встановіть мобільний антивірус і програмне забезпечення для захисту даних.

– Регулярно оновлюйте операційну систему та програмне забезпечення на своєму пристрої.

2. Захист даних:

– Не зберігайте конфіденційні дані, такі як паролі, номери кредитних карток або медичні записи, на своєму мобільному пристрої, якщо це абсолютно необхідно.

– Зберігайте важливі дані за допомогою зашифрованого хмарного сховища.

– Шифруйте конфіденційні файли, перш ніж надсилати їх комусь.

– Будьте обережні з загальнодоступними мережами Wi-Fi, оскільки вони можуть бути небезпечними.

– Завантажуйте додатоки тільки з офіційного магазину додатків.

3. Секретність:

– Перевірте налаштування конфіденційності програми або пристрою, щоб переконатися, що ваші дані не передаються без вашого відома.

– Вимкніть служби геолокації, якщо вони не використовуються.

– Слідкуйте за інформацією, яку Ви публікуєте в соціальних мережах та інших онлайн-платформах.

– Не відкривайте підозрілі посилання або повідомлення електронної пошти або SMS.

4. Резервне копіювання та відновлення:

– Регулярно створюйте резервні копії даних на своєму комп'ютері або в хмарному сховищі.

– Зберігайте резервну копію окремо від мобільного пристрою в надійному місці.

– Перегляньте план відновлення мобільного оператора або виробника пристрою, щоб дізнатися, що робити, якщо пристрій втрачено або пошкоджено.

Будь ласка, пам'ятайте:

– Ви несете відповідальність за захист даних на своєму мобільному пристрої.

– Вживайте необхідних заходів для захисту вашого пристрою та даних,

– Остерігайтеся онлайн-загроз,

– Регулярно створюйте резервні копії [3].

Дотримуючись цих порад, ви можете зберегти свої дані в безпеці та конфіденційності на своєму мобільному пристрої.

Висновки. Війна в Україні ставить перед суспільством безліч проблем, однією з яких є захист персональних даних. З одного боку, держава вимагає певних обмежень щодо прав громадян на захист і підтримання громадського порядку. З іншого боку, громадяни мають право на недоторканність приватного життя та захист від незаконного збору, використання та розповсюдження персональних даних.

Інформаційні джерела

1. Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk/
2. Чому хмара може бути найбезпечнішим місцем для зберігання конфіденційних даних. URL: https://zepcam.com/uk/%D1%87%D0%BE%D0%BC%D1%83-%D1%85%D0%BC%D0%B0%D1%80%D0%B0-%D0%BC%D0%BE%D0%B6%D0%B5-%D0%B1%D1%83%D1%82%D0%B8-%D0%BD%D0%B0%D0%B9%D0%B1%D 0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%BD%D1%96%D1%88%D0%B8%D0%BC-%D0%BC/
3. Захист мобільних даних допоможе вберегтися від зловмисників. URL: https://www.microsoft.com/uk-ua/microsoft-365/business-insights-ideas/resources/how-mobile-data-protection-can-help-keep-intruders-out

УДК 004.056

КІБЕРЗАГРОЗИ ПІД ЧАС ВІЙНИ: ТАКТИКИ, МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ

Анна-Марія-Іванна ПАНЬКІВ
Олександр ХЛЕВНОЙ
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The article examines the main tactics and methods of cyberthreats during military conflicts and modern approaches to counteract them. Special attention is paid to the use of artificial intelligence, big data analytics, and cloud technologies for securing information systems.*

Keywords*: cybersecurity, war, cyberthreats, defense methods, information security.*

Анотація. *У статті досліджено основні тактики та методи кіберзагроз під час військових конфліктів та сучасні підходи до їх нейтралізації. Особливу увагу приділено використанню штучного інтелекту, аналітики великих даних та хмарних технологій для забезпечення захисту інформаційних систем.*

Ключові слова*: кібербезпека, війна, кіберзагрози, методи захисту, інформаційна безпека.*

У сучасних умовах військові конфлікти перетворюються на багатовимірні протистояння, в яких кіберзагрози стали одним із ключових інструментів для досягнення стратегічних цілей. Атаки на інформаційні системи державних установ, критичної інфраструктури та комерційних компаній можуть мати серйозні наслідки як для безпеки країни, так і для її економіки.

Сучасні військові конфлікти висувають нові вимоги до кібербезпеки, змушуючи держави і організації шукати способи захисту від різноманітних і

складних кіберзагроз. Кіберпростір використовується зловмисниками як платформа для проведення шпигунських операцій, дезінформаційних кампаній та атак на критичну інфраструктуру.

Актуальні підходи та технології в кіберзахисті під час війни включають в себе:

– Кіберрезилентність систем, яка забезпечує стійкість до атак і здатність відновлюватися після інцидентів. Це підхід, при якому системи спроектовані так, щоб зберігати працездатність навіть під час кібератак.

– Оперативна кіберрозвідка, яка проводить збір і аналіз інформації про потенційні загрози та їхні джерела. Це дозволяє передбачати можливі сценарії атак і вживати превентивних заходів.

– Технології сегментації мережі, які обмежують доступ до певних частин інфраструктури для запобігання розповсюдженню шкідливого програмного забезпечення. Це дозволяє ізолювати заражені системи та захистити інші важливі компоненти.

– Автономні системи реагування, які не тільки виявляють, але й автоматично блокують атаки, запобігаючи їх подальшому розвитку. Використання автоматизованих платформ забезпечує мінімізацію часу реакції на загрози.

– Використання honeypot-систем, які призначені для відволікання та виявлення кіберзловмисників з фіктивних серверів і мереж. Такі системи дозволяють вивчати поведінку атакуючих та з'ясовувати нові методи і техніки.

Сучасні тенденції також включають розвиток Zero Trust підходу, де кожен запит на доступ до ресурсів розглядається як потенційно небезпечний, незалежно від того, чи надходить він з внутрішньої мережі, чи ззовні. Це значно ускладнює зловмисникам доступ до критично важливих даних.

До основних типів кіберзагроз включають:

– DDoS-атаки, спрямовані на перевантаження серверів і призупинення роботи онлайн-сервісів.

– Фішингові кампанії, що допомагають зловмисникам отримати доступ до конфіденційної інформації через обман користувачів.

– Віруси-вимагачі, які блокують доступ до систем і вимагають викуп за розблокування.

– Шпигунські програми, що непомітно збирають інформацію для подальшого використання у військових цілях.

В сучасній системі захисту методи та технології спрямовані на швидке виявлення і нейтралізацію загроз. Тому основні технології, що застосовуються для цього, включають в себе:

– Штучний інтелект (ШІ), який використовується для автоматизації процесів моніторингу та аналізу. Алгоритми ШІ можуть ідентифікувати аномальну активність у мережах, що дозволяє своєчасно реагувати на загрози.

– Аналітика великих даних, яка дає можливість аналізувати великі обсяги даних, які генеруються під час роботи систем. Це допомагає виявити патерни поведінки, що можуть свідчити про потенційну загрозу.

– Хмарні технології, які забезпечують резервне копіювання даних і можливість їх відновлення у разі кібератаки. Хмарні платформи також дозволяють забезпечити додатковий рівень безпеки завдяки ізоляції критично важливих даних від місцевих систем.

Висновки. Отже, кіберзагрози під час військових конфліктів стали значним викликом для державної безпеки та економіки. Ефективне управління кібербезпекою потребує комплексного підходу, що включає застосування штучного інтелекту, аналітики великих даних та хмарних технологій для виявлення і блокування загроз. Використання методів кіберрозвідки та підходу Zero Trust підвищує стійкість систем. Тому поєднання сучасних технологій та підготовки спеціалістів забезпечує надійний захист інформаційних систем у складних умовах.

Інформаційні джерела

1. Brown A., & Lee S. (2021). "AI-Powered Solutions for Cyber Defense". Journal of Cybersecurity Studies, 15(3), pp. 245–258.

2. Kovalenko D. (2023). "Strategies for Cybersecurity in Conflict Zones". Cybersecurity Review, 28(4), pp. 180–193.

3. Smith J. (2022). Cybersecurity in Modern Warfare. New York: TechPress.

4. Гринько В. І. (2023). Сучасні методи управління кібербезпекою в умовах війни. Збірник наукових праць, 32, С. 15–22.

УДК: 004.738.5:351.861

ДОСЛІДЖЕННЯ СУЧАСНИХ КОМУНІКАЦІЙНИХ ПЛАТФОРМ ДЛЯ ОПТИМІЗАЦІЇ ТА АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ПОВСЯКДЕННОЇ ДІЯЛЬНОСТІ ДСНС УКРАЇНИ

Еміль БИК
Назарій БУРАК
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *In the work, modern communication platforms for optimizing and automating the everyday activities of the State Emergency Service of Ukraine (SES) are studied. The use of cloud solutions, automated task management, and data protection measures are analyzed, focusing on their impact on enhancing operational efficiency and minimizing risks during emergency response.*

Keywords: *SES, communication platforms, automation, information security, cloud technologies.*

Анотація. *У роботі досліджуються сучасні комунікаційні платформи, що використовуються для оптимізації та автоматизації діяльності Державної служби України з надзвичайних ситуацій (ДСНС). Розглядаються можливості впровадження хмарних рішень, автоматизованого управління завданнями, а також заходів з інформаційної безпеки для забезпечення ефективної координації дій та захисту критично важливих даних. Особлива увага приділяється впливу цих технологій на підвищення оперативності реагування та мінімізацію ризиків під час ліквідації наслідків надзвичайних ситуацій.*

Ключові слова: *ДСНС, комунікаційні платформи, автоматизація, інформаційна безпека, хмарні технології.*

Розвиток сучасних інформаційних технологій надає широкі можливості для вдосконалення комунікаційних процесів, особливо в контексті діяльності Державної служби України з надзвичайних ситуацій (ДСНС). Застосування новітніх технологій забезпечує не тільки покращення координації рятувальних операцій, але й автоматизацію рутинних завдань, що дозволяє зменшити навантаження на персонал і підвищити ефективність роботи. У цьому контексті дослідження фокусується на аналізі комунікаційних платформ, які можуть бути застосовані для оптимізації процесів в умовах надзвичайних ситуацій.

Одним із ключових аспектів є використання хмарних рішень для зберігання та оперативного обміну даними. Хмарні платформи забезпечують безпечне управління інформацією, що є надзвичайно важливим у критичних ситуаціях. Інтеграція систем моніторингу та контролю ресурсів у реальному часі дозволяє рятувальним підрозділам швидко отримувати інформацію про поточні умови на місці подій та приймати обґрунтовані рішення. Такі рішення також сприяють автоматизації повідомлень та оновлень, що зменшує навантаження на персонал і мінімізує ризик людських помилок.

Удосконалені методи автентифікації, зокрема багатофакторна аутентифікація, є важливою частиною заходів із захисту інформації. Вони забезпечують захист від несанкціонованого доступу до чутливої інформації, що особливо важливо при обміні даними між різними структурними підрозділами ДСНС і зовнішніми партнерами. Крім того, системи автоматичних сповіщень про спроби несанкціонованого доступу сприяють оперативному реагуванню на загрози.

Сучасні комунікаційні платформи також сприяють автоматичному розподілу завдань серед рятувальників, їхньому моніторингу та оновленню статусів операцій у реальному часі. Такі рішення можуть бути інтегровані із системами GPS-навігації, що дає змогу забезпечити точну координацію дій та мінімізувати затримки під час реагування на надзвичайні ситуації. Це

особливо важливо для ефективного управління великими командами та забезпечення швидкого виконання завдань.

Використання геоінформаційних систем (ГІС) дозволяє оперативно оцінювати масштаби катастрофи та прогнозувати її розвиток. Вони також сприяють плануванню розподілу ресурсів, що підвищує ефективність рятувальних операцій та знижує можливі втрати. ГІС надають змогу візуалізувати інформацію, що дозволяє приймати обґрунтовані рішення на основі точних даних про місце подій.

Рис. 1. Ключові аспекти вдосконалення комунікаційних процесів

Серед сучасних комунікаційних платформ, що використовуються для координації рятувальних операцій, варто зазначити ***Discord, WhatsApp та Signal.*** Кожна з цих платформ має свої переваги та обмеження, але *Discord* вирізняється широкими можливостями для організації багатоканальної комунікації, а також має найкращу підтримку інтеграцій з іншими сервісами та інструментами автоматизації. Платформа підтримує текстові, голосові та відео повідомлення, що дозволяє забезпечити різноманітні способи взаємодії в команді. З огляду на це, Discord є найкращим вибором для забезпечення ефективної координації під час рятувальних операцій.

WhatsApp, попри свою популярність серед користувачів, має обмеження у контексті складних комунікаційних задач, оскільки не підтримує багатоканальну організацію чатів та інтеграції з іншими інструментами. У той же час *Signal*, хоча й має найвищий рівень захисту даних завдяки шифруванню, також обмежений у функціях, що стосуються управління командною роботою та інтеграції з іншими платформами.

Висновки. У роботі обґрунтовано важливість впровадження сучасних інформаційних технологій у діяльність Державної служби України з надзвичайних ситуацій (ДСНС). Доведено, що автоматизація процесів і використання захищених комунікаційних платформ значно підвищують ефективність управління та реагування на надзвичайні ситуації. Це дозволяє забезпечити оперативне прийняття обґрунтованих рішень, знижуючи ризики для життя і здоров'я людей. Зокрема, використання таких платформ, як Discord, у поєднанні з хмарними рішеннями та геоінформаційними системами, ство-

рює умови для швидкого обміну даними, оптимізації координації дій та покращення інформаційної безпеки. Впровадження цих технологій сприятиме ефективнішому управлінню рятувальними операціями та підвищенню загальної готовності до ліквідації катастроф.

Інформаційні джерела

1. Кочубей Л. Особливості сучасних інформаційнокомунікативних технологій в Україні: наукові записки. URL: https://ipiend.gov.ua/wp-content/ uploads/2018/07/ kochubei_osoblyvosti.pdf

2. Швачич Г. Г., Толстой В. В., Петречук Л. М., Іващенко Ю. С., Гуляєва О. А., Соболенко О. В. Сучасні інформаційно-комунікаційні технології. URL: https:// nmetau.edu.ua/file/ikt_tutor.pdf

3. Наголюк М. Сучасні інформаційно-комунікаційні технології у підготовці прикордонників молодшої ланки в країнах Європейського Союзу. URL: https:// www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://od.kubg.edu.ua/ index.php/journal/article/download/1105/883/3510&ved=2ahUKEwjBlpnOh-aJAxVjHhAI HQf2OXUQFnoECC0QAQ&usg=AOvVaw0xjo6DVGPD7R4meH5g-Mou

УДК 65.01: 658

ПРОЦЕСНИЙ ПІДХІД В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВАХ, ЯКІ НАДАЮТЬ ІТ-ПОСЛУГИ

Ярослав ВОДОНІС
Орест ПОЛОТАЙ
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The features of implementing information security management at enterprises using a process approach are described.*
Keywords: *information security, IT services, process approach.*

Анотація. *Описано особливості реалізації управління інформаційною безпекою на підприємствах з використанням процесного підходу.*
Ключові слова: *інформаційна безпека, ІТ-послуги, процесний підхід.*

Управління інформаційною безпекою (ІБ) – важливий вид діяльності, метою якого є контроль процесів забезпечення інформацією та запобігання її несанкціонованому використанню. Керівники організації приймають рішення щодо явного чи опосередкованого управління інформацією, оптимізувати ці процеси можливо при детальному аналізі ризиків. Цей аналіз визначить вимоги до інформаційної безпеки та буде вхідною інформацією для підсистеми управління інформаційною безпекою організації.

Вимоги бізнесу до забезпечення ІБ впливають на постачальників інформаційних послуг і мають бути закладені в нормативних документах організації, зокрема в "Угодах про рівень Сервісу". Процес управління ІБ полягає у постійному забезпеченні безпеки послуг на узгодженому із замовником послуг рівні. Безпека є найважливішим показником якості управління.

Процес управління ІБ полягає в інтеграції аспектів безпеки в організації з точки зору постачальника інформаційних послуг та забезпечує комплекс документів та заходів щодо розробки, ведення та оцінки заходів безпеки.

Традиційний технологічний підхід у своїй основі насамперед концентрується на самих технологіях, а в основі IT Service Management (ITSM) підходу управління інформаційними послугами розташований клієнт та його потреби в послугах, що надаються за допомогою інформаційних технологій. Причому даний підхід поєднує в собі процесну організацію надання послуг та зафіксовані в угодах про рівень послуг ключові показники ефективності (Key Performance Indicators, KPI), що говорить про системність, вимірюваність та контрольованість якості надання послуги та відповідно до керованості даного процесу.

IT Service Management (ITSM) – управління IT-послугами. Впровадження та управління якісними IT-послугами, які відповідають потребам бізнесу. Управління IT-послугами реалізується постачальниками IT-послуг шляхом використання найбільш оптимального поєднання людей, процесів та інформаційних технологій.

Основу ITSM – складає сукупність із десяти основних процесів, описаних у томах ServiceSupport та ServiceDelivery бібліотеки ITIL – комплексу документів– IT Infrastructure Library [1]:

– управління інцидентами (Incident management);
– управління проблемами (Problem management);
– управління конфігураціями (Configuration management);
– управління змінами (Change management);
– управління релізами (Release management);
– управління рівнем сервісу (Service Level Management);
– управління фінансами (Financial management for IT services);
– управління доступністю (Availability management);
– управління безперервністю (IT service continuity management);
– управління потужністю (Capacity management).

Необхідно вибудовувати управління службою ІБ на основі процесного підходу, за умови, що ця служба складається з більш ніж одного-двох співробітників. Служба ІБ має бути вбудована у процеси управління та інтегрована з ними. У свою чергу, керівнику, який відповідає за ІБ, необхідно брати участь у процесах, що відбуваються в організації, іноді навіть очолюючи їх, якщо це необхідно для забезпечення ІБ на всіх етапах, починаючи від розробки та закінчуючи впровадженням та подальшим виведенням з експлуатації

та знищенням тих чи інших процесів та систем. Необхідно не тільки дивитися на свою ділянку роботи, але й розуміти архітектуру рішень та бізнес-вимоги, а також впливати на них, якщо бачиш, що рішення може бути невірним чи неоптимальним.

Орієнтація підрозділу ІБ на надання бізнесу якісних послуг з управління ризиками ІБ, забезпечення відповідності вимогам ІБ та організації процесів ІБ є важливою частиною підходу до корпоративного управління та інтеграції функції ІБ в загальну структуру бізнесу компанії. Для бізнес-підрозділів інформаційна безпека стає однією з важливих споживаних послуг, спрямованої на підвищення надійності та безпеки бізнесу та зниження різних витрат, пов'язаних із ризиками ІБ. При цьому захист інформаційних активів компанії, власниками яких є бізнес-підрозділи, стає послугою, що надається їм підрозділом ІБ [2].

У сервісній моделі надання послуг всі сервіси описані, деталізовані, для кожного сервісу є свої метрики, за кожним співробітником служби інформаційної безпеки закріплено роль та визначено частку участі у певному сервісі, розраховано собівартість сервісів та тарифи, визначено KPI, за допомогою яких можна відстежувати відповідність сервісу закріпленому у SLA рівню.

Результатом діяльності підрозділу ІБ не може бути набір послуг, оскільки послуги, що надаються підрозділом, в результаті спрямовані на захист активів організації, на запобігання фінансовим і репутаційним збиткам, тому для бізнес-підрозділів важлива розумна впевненість у тому, що рівень ризиків ІБ прийнятний для бізнесу. А якщо розглядати з погляду сервісної моделі надання послуг, то результатом діяльності служби ІБ є виконання зафіксованого у SLA рівня сервісу.

Безпека – це постійний процес, а якраз і вимагає постійного чи періодичного виконання певних дій, які можна реалізовувати у вигляді послуги ІБ. Серед таких послуг можуть бути і ті, що надаються внутрішніми підрозділами, та послуги від зовнішніх постачальників. Як розподілити, що і кому довірити, – це залежить від моделі загроз конкретних підприємств.

До послуг ІБ, як і до інших послуг, пов'язаних з ІТ, можуть бути успішно застосовані рекомендації ITSM – *наприклад*, з управління рівнем послуги та моніторингу основних її параметрів, формалізація яких здійснюється під час укладання SLA з бізнес-підрозділами. Для послуги ІБ такими параметрами є забезпечення конфіденційності, цілісності та доступності. Для реалізації комплексної системи управління інформаційною безпекою відповідно до кращих практик управління ІБ, викладених у стандартах серії ISO 27000, необхідно використовувати цикл Демінгу та процесний підхід.

При визначенні списку процесів, які у службі ІБ слід побудувати насамперед, слід відштовхуватися від результатів аналізу ризиків ІБ у конкретній організації [3]. Зазвичай найбільш критичні процеси управління правами доступу, забезпечення конфіденційності та управління інцидентами ІБ.

Це базис, на основі якого необхідно загалом вибудовувати процес забезпечення ІБ. Звичайно, потрібна і деталізація процесів усередині служби, щоб розуміти, які з них низькоефективні, які вимагають великих трудовитрат при невеликій віддачі, які базуються на виконанні рутинних операцій і вимагають автоматизації.

До найбільш критичних процесів належать "управління доступом, управління ризиками ІБ, аналіз ефективності ІБ, аудит процесів ІБ, забезпечення безперервності ІТ-сервісів та резервне копіювання, а також управління інцидентами ІБ" [5].

Не слід забувати про процес регулярної професійної перепідготовки служб ІБ (щоб вони не втрачали адекватності в аналізі ситуації та професійно реагували на інциденти – оскільки зараз питання зазвичай полягає не в тому, чи станеться інцидент, а в тому, коли це буде і наскільки оперативно грамотно на нього зреагує компанія) і підвищення знань про ІБ у звичайних користувачів [4].

Застосування процесного підходу до реалізації процесів управління ІТ та ІБ дозволяє вибудувати інтегровану систему управління ІТ-ризиками, що поєднує в собі процеси управління ризиками ІБ (відповідно до ISO 27000), ризиками управління ІТ-сервісами (на основі ISO 20000 та ITIL) та ризиками переривання бізнесу (за стандартами BS 25999, BS 25777 та ISO 22301).

Компаніям та службам інформаційної безпеки корисно мати каталог послуг ІБ. Каталог послуг може мати багаторівневу структуру. У дворівневому каталозі сервісів ІБ Перший рівень визначає сервіс, що надається, другий рівень розбиває його на окремі послуги. Цілком сервіс може бути не дуже цікавий бізнес-підрозділам, але окремі послуги, що входять до нього, надзвичайно потрібні.

Висновки. Як бачимо, процесний підхід дозволяє гармонійно будувати діяльність служб ІБ. Дуже важливо щоб цей процес відповідав ключовим принципам, на яких будується процесне управління організацією в цілому. Підсумком цих зусиль стане набагато чіткіша і зрозуміліша для бізнесу робота, націлена на результат, який можна виміряти за заздалегідь узгодженими показниками.

Інформаційні джерела

1. Веб-сайт "ITIL & ITSM World". URL: http://www.itil-itsm-world.com

2. Інформаційна безпека компанії: 10 правил для бізнесу і працівників. URL: https://biz.ligazakon.net/news/214929_nformatsyna-bezpeka-kompan-10-pravil-dlya-bznesu--pratsvnikv

3. Кухарська Н. П., Полотай О. І. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. Information Technology and Security. July-December 2019. Vol. 7. Issue. 2 (13), pp. 126–136.

4. Полотай О. І. Сусяк Р. Я. Особливості проекту підвищення рівня обізнаності працівників підприємств в сфері кібербезпеки. "Світ наукових досліджень" (матеріали

Міжнародної мультидисциплінарної наукової інтернет-конференції (м. Тернопіль, Україна, м. Ополе, Польща, 23–24 квітня 2024 р.). Вип. 29. – С. 257–259.

5. Ящук В. І., Полотай О. І., Тичина Ю. Модель системи управління інцидентами інформаційної безпеки. Зб. тез доп. V Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів "Інформаційна безпека та інформаційні технології". (м. Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. – С. 108–111.

УДК: 004.056:343.98

ЦИФРОВА КРИМІНАЛІСТИКА

Роман ЛИТВИНЕНКО
Василь ЛУЧИК

Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The paper examines digital forensics as a tool for collecting and analyzing digital evidence. The key methods, current challenges, and capabilities of the EnCase Forensic tool are described. The focus is on the legal aspects of using digital evidence in criminal proceedings in Ukraine.*

Keywords: *digital forensics, digital evidence, EnCase Forensic, cybercrime, legal regulation, electronic documents.*

Анотація. *У роботі розглянуто цифрову криміналістику як інструмент для збору та аналізу цифрових доказів. Описуються ключові методи, сучасні виклики та можливості інструменту EnCase Forensic. Акцентується увага на правових аспектах використання цифрових доказів у кримінальному провадженні України.*

Ключові слова: *цифрова криміналістика, цифрові докази, EnCase Forensic, кіберзлочинність, правова регламентація, електронні документи.*

Цифрова криміналістика – це спеціалізована галузь криміналістики, яка зосереджується на виявленні, зборі, аналізі та поданні цифрових доказів. Вона охоплює методи розслідування злочинів, пов'язаних із використанням комп'ютерів, мобільних пристроїв та інших цифрових технологій. Цифрова криміналістика виникла у 1980-х роках як відповідь на зростання злочинів, що залучали комп'ютерні системи, і з того часу розвивалася відповідно до потреб суспільства. Її мета – забезпечити докази для судового процесу або оперативно-розшукових заходів, особливо у сфері кіберзлочинності, де традиційні методи виявлення злочинців є недостатніми. Зростання впровадження цифрових технологій у повсякденне життя зробило цифрову криміналістику важливим інструментом для боротьби з кіберзлочинами. Вона дозволяє відслідковувати цифрові сліди, залишені підозрюваними, аналізувати мережеву активність, виявляти компрометуючі файли та інші електронні докази.

У випадках кіберзлочинів, таких як шахрайство, витік даних або кібербулінг, цифрові докази можуть бути вирішальними для встановлення причетності або непричетності підозрюваних. У судах вони слугують як прямими доказами (*наприклад*, текстові повідомлення), так і непрямими (метадані, геолокація). Цифрова криміналістика базується на загальновизнаних принципах збереження доказів, таких як недоторканість, достовірність і можливість повторного відтворення результатів аналізу. Збір доказів включає виявлення цифрових слідів, *наприклад*, активних (дані, залишені користувачами навмисно, як-от пости у соцмережах) та пасивних (ненавмисно створені дані, такі як історія браузера).

Для забезпечення надійності цифрових доказів використовуються спеціалізовані інструменти для копіювання, зберігання та аналізу інформації без її модифікації. Основною метою роботи з доказами є доведення їх автентичності та правомірності для використання у суді або під час слідства. З розвитком технологій з'явилися нові виклики, такі як робота з хмарними сервісами, пристроями Інтернету речей (IoT) та мобільними додатками. Сучасні підходи до цифрової криміналістики вимагають не лише технічних знань, але й врахування правових аспектів, *наприклад*, захисту персональних даних. Крім того, наявність складних цифрових моделей, як-от Загальна модель комп'ютерних криміналістичних розслідувань (GCFIM), сприяє стандартизації процесів розслідування, що дозволяють підвищити ефективність роботи слідчих, надаючи їм методики для роботи з різноманітними цифровими пристроями та середовищами.

Цифрова криміналістика оперує широким спектром даних, які можуть слугувати доказами у розслідуваннях. До таких даних належать: метадані, електронні листи, повідомлення та чати, зображення, а також логи. Метадані – це інформація про файли, що включає дату створення, останнього редагування, геолокацію, тип пристрою, вони дозволяють відновити хронологію подій і підтвердити автентичність доказів.

Зміст електронних листів складається зі списків адресатів та метаданих, що часто стають важливими доказами у справах про шахрайство, зловживання службовим становищем або змови. Повідомлення та чати, тобто дані, отримані з месенджерів, таких як WhatsApp або Telegram, дозволяють розкрити спілкування між підозрюваними. Зображення є аналізом цифрових фото, що може включати перевірку метаданих, геотегів і навіть визначення маніпуляцій із зображенням. Логи – це журнали активності систем, зокрема дані про відвідані веб ресурси, входи в систему або інші дії, можуть вказувати на поведінку користувача та допомогти в розслідуванні.

EnCase Forensic є потужним інструментом, який використовується у цифровій криміналістиці для збору, аналізу та збереження цифрових доказів. Аналіз та відновлення даних, EnCase підтримує різні файлові системи (FAT, NTFS, exFAT тощо) та формати копій носіїв (DD, E01). Завдяки сигнатурному аналізу програма може відновлювати видалені файли, зберігаючи

їхні повні шляхи. Робота з поштою та повідомленнями, програма дає змогу отримувати електронні листи та повідомлення з популярних месенджерів, що є критично важливим для відновлення діалогів і перевірки достовірності листування. Media Analyzer у складі EnCase використовує технологію візуального розпізнавання для швидкої фільтрації зображень, зокрема тих, що містять ключові докази. EnCase забезпечує збереження ланцюга доказів, використовуючи хешування за алгоритмами MD5 та SHA-1. Це гарантує, що докази не змінювалися з моменту їх отримання.

Програма дозволяє автоматизувати багато процесів, зокрема пошук за ключовими словами, перегляд вкладених файлів та отримання даних із хмарних сховищ, таких як Microsoft O365 і SharePoint. Такий комплексний підхід сприяє підвищенню ефективності розслідування та дозволяє криміналістам зосередитися на аналізі отриманої інформації. Завдяки своїй гнучкості EnCase є універсальним інструментом, який допомагає працювати з цифровими доказами, зберігаючи їхню автентичність і придатність для використання у судових процесах. Його застосування дозволяє швидко отримати доступ до необхідної інформації, виявити сліди злочинної діяльності та створити детальні звіти для представлення у суді. Це робить EnCase Forensic важливим елементом сучасної цифрової криміналістики.

Цифрові докази стали невід'ємною складовою сучасного кримінального провадження, але їхня правова регламентація ще перебуває на етапі розвитку. Згідно з чинним Кримінальним процесуальним кодексом України (КПК), статус електронних документів і доказів не має чіткої визначеності. Відсутність у законодавстві термінів "цифровий доказ" та "електронний документ" ускладнює процес їх належного оформлення та використання у судовій практиці. Суди часто базуються на формальних вимогах до оформлення протоколів огляду Інтернет-ресурсів або цифрових носіїв, проте це не вирішує питання систематизації та однаковості підходів у доказуванні. Етичні аспекти цифрової криміналістики включають дотримання прав людини під час збирання доказів, уникнення порушення приватності та забезпечення точності інформації.

Наприклад, дані, отримані з мережі Інтернет, мають бути зібрані відкрито, якщо це можливо, без порушення конфіденційності. Принципи, закладені в міжнародних стандартах, таких як Протокол Берклі, підкреслюють необхідність професійного підходу до збору, зберігання та використання цифрової інформації. Це особливо важливо, коли йдеться про випадки, пов'язані із злочинами, вчиненими в умовах воєнного стану або на тимчасово окупованих територіях. Важливим аспектом використання цифрових доказів є забезпечення їхньої автентичності та збереження цілісності. Протоколи огляду, технічна фіксація та відповідне зберігання надійно захищають дані від маніпуляцій. Використання сучасних технологій, таких як хешування за алгоритмами MD5 або SHA-1, дозволяє забезпечити надійну перевірку

оригінальності файлів. Проте навіть такі інструменти мають супроводжуватися юридичною відповідністю всіх дій вимогам КПК.

Висновки. У практиці це означає не лише фіксацію процесуальних дій, але й дотримання вимог до змісту та форми електронних документів. Міжнародні практики демонструють важливість інтеграції цифрових доказів у процесуальні кодекси. *Наприклад*, у багатьох країнах електронні документи вже визнаються процесуальними доказами завдяки наявності чітких стандартів їх оформлення та подання до суду. Україна, поступово запроваджуючи такі норми, має взяти за основу досвід розвинених країн та адаптувати його до своїх умов, що передбачає закріплення у КПК поняття "цифрові докази", розробку методик роботи з ними, а також підвищення кваліфікації правоохоронців у цій сфері.

Інформаційні джерела

1. Цифрова криміналістика: проблеми теорії і практики. URL: http://lsej.org.ua/4_2022/90.pdf (дата звернення: 15.11.2024).

2. Використання цифрової інформації в розслідуванні кримінальних правопорушень. URL: https://ivpz.kh.ua/wp-content/uploads/2023/01/%D0%97%D0%B1%D1% (дата звернення: 14.11.2024).

3. EnCase Forensic. URL: https://cybermarket.com.ua/product/encase-forensic/ (дата звернення: 13.11.2024).

4. Теоретичні та праксеологічні аспекти фіксування та використання у кримінальному процесуальному доказуванні інформації з інтернет-джерел. URL: http://lsej.org.ua/10_2022/194.pdf (дата звернення: 16.11.2024).

УДК 351.74:343.9

КРИМІНАЛЬНО-ПРАВОВІ ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У КІБЕРПРОСТОРІ ТА ЕКСПЕРТНА РОЛЬ ГРОМАДСЬКИХ (НЕУРЯДОВИХ) ОРГАНІЗАЦІЙ

Іван МУКАН [1]
Ольга КОТОВСЬКА [2]

[1]***Кафедра права Львівського національного університету природокористування, м. Львів, Україна.***

[2]***Кафедра адміністративного та фінансового менеджменту Національного університету "Львівська політехніка", м. Львів, Україна.***

Abstract. *The article analyzes the legal and organizational principles of ensuring security in cyberspace in light of international and national legislation. It examines the key provisions of the Convention on Cybercrime, the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", and the norms of the Criminal Code of Ukraine. The article proposes enhancing the effectiveness of combating cybercrime by involving non-governmental organizations specializing in cybersecurity and information technology.*

Keywords: *cyberspace, cybercrime, public non-governmental organizations, cybersecurity.*

Анотація. *У статті проаналізовано правові та організаційні засади забезпечення безпеки у кіберпросторі у світлі міжнародного та національного законодавства. Розглянуто основні положення Конвенції про кіберзлочинність, Закону України "Про основні засади забезпечення кібербезпеки України" та норм Кримінального кодексу України. Запропоновано підвищення ефективності боротьби з кіберзлочинністю шляхом залучення громадських (неурядових) організацій, які спеціалізуються у сфері кібербезпеки та інформаційних технологій.*

Ключові слова: *кіберпростір, кіберзлочин, громадські (неурядові) організації, кібербезпека.*

Сучасне суспільство вже не уявляє свого життя без інтернету, комп'ютерів, смартфонів та інших цифрових пристроїв. На рівні з реальним простором розвивається кіберпростір, який у майбутньому може повністю полонити більшість сфер нашого життя. Все це є наслідками цифрової революції, яка відбувається завдяки розвитку інформаційно-телекомунікаційних технологій. Активний розвиток кібертехнологій та IT-бізнесу в останні роки так само активно спонукає і можливості для вчинення злочинів онлайн та у сфері інформаційних технологій. У всьому світі злочини у кіберпросторі щороку завдають збитків на десятки мільярдів доларів США як державам, так і приватним компаніям. З іншого боку, російсько-українська війна та її гібридний характер включає кіберскладову, зокрема кібероперації та використання кібератак заради отримання переваги чи завдання шкоди шляхом втручання у систему державних або приватних установ, що посилює відповідальність за дії у цифровому просторі.

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [1].

Відповідно до викликів сучасності необхідно враховувати наявне кримінально-правове регулювання правовідносин у кіберпросторі. Кіберзлочинність безумовно стає небезпекою XXI сторіччя, а відтак кібербезпека набуває значення нарівні з фізичною безпекою, адже товщина сталевих дверей сховища перестає бути важливою, якщо сховище можна відкрити за допомогою комп'ютерної системи.

У 2001 році 35 держав (країни Ради Європи, а також Австралія, Домініканська Республіка, Японія, Панама, США) прийняли Конвенція про кіберз-

лочинність, яку Україна ратифікувала 07.09.2005. Конвенція про кіберзлочинність стала основою для гармонізації національного законодавства у сфері кіберпростору, яка продовжується і зараз.

Конвенція спрямована на доповнення існуючих конвенцій Ради Європи щодо співробітництва у кримінальній сфері, а також аналогічних угод між державами-членами Ради Європи та іншими країнами. Її мета – підвищити ефективність кримінальних розслідувань і судових переслідувань, пов'язаних із правопорушеннями, що стосуються комп'ютерних систем та даних. Окрім того, Конвенція створює правові умови для збору доказів у кримінальних справах, зокрема в електронній формі, що сприяє вдосконаленню міжнародного співробітництва у протидії кіберзлочинності.

Конвенцією запропоновано поділяти кіберзлочини на наступні види:

– правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ до систем; нелегальне перехоплення інформації; втручання у дані та системи; виготовлення, розповсюдження та збут шкідливого програмного забезпечення та спеціальних пристроїв);

– правопорушення, пов'язані з комп'ютерами (комп'ютерне підроблення та комп'ютерне шахрайство);

– правопорушення, пов'язані зі змістом (вироблення, володіння, розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем);

– правопорушення, пов'язані з порушенням авторських та суміжних прав [2].

В Україні кіберпростір регулюється значною кількістю нормативно-правових актів. До основних варто віднести Закони України "Про основні засади забезпечення кібербезпеки України", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про захист персональних даних", "Про ратифікацію Конвенція про кіберзлочинність", Кодекс України про адміністративні правопорушення, а також Кримінальний і Кримінальний Процесуальний Кодекси України.

Правові та організаційні основи забезпечення захисту інтересів у кіберпросторі в Україні визначено у Законі України "Про основні засади забезпечення кібербезпеки України". Відповідно до зазначеного закону запроваджено державно-приватну взаємодія у сфері кібербезпеки, яка серед іншого здійснюється шляхом тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі [1].

У чинному Кримінальному кодексі України наявно 7 статей, які визначають відповідальність за кіберзлочини:

1. Незаконне відтворення, використання та розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, інших

творів, а так само незаконне відтворення, використання та розповсюдження виконань, фонограм, відеограм і програм мовлення, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації, камкординг, кардшейрінг або інше умисне порушення авторського права і суміжних прав, а також фінансування таких дій, якщо це завдало матеріальної шкоди у значному розмірі. (ст.176 КК України).

Матеріальна шкода вважається завданою в значному розмірі, якщо її розмір у двадцять і більше разів перевищує неоподатковуваний мінімум доходів громадян, у великому розмірі – якщо її розмір у двісті і більше разів перевищує неоподатковуваний мінімум доходів громадян, а завданою в особливо великому розмірі – якщо її розмір у тисячу і більше разів перевищує неоподатковуваний мінімум доходів громадян.

2. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. (ст.361 КК України);

3. Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. (ст.361^1 КК України);

4. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства. (ст.361^2 КК України);

5. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї. (ч.1 ст.362 КК України);

6. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації. (ч.2 ст.362 КК України);

7. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. (ст.363 КК України) [3].

На сьогоднішній день в Україні, як і в світі в цілому, рівень кібербезпеки явно недостатній. Міжнародна співпраця сприяє вирішенню цієї проблеми,

однак основні зміни повинні бути здійснені в середині країни, щоб згодом передати світу наш успішний досвід боротьби з кіберзлочинністю і регулювання кіберпростору. Для цього держава і суспільство повинно об'єднати свої зусилля та зробити все можливе для подолання проблеми кіберзлочинності.

Висновки. На нашу думку залучення до вирішення цієї проблеми громадських (неурядових) організацій, які спеціалізуються у сфері кібербезпеки та інформаційних технологій дасть змогу пришвидшити виявлення та підняти рівень боротьби з правопорушеннями у кіберпросторі на якісно вищий рівень.

Інформаційні джерела

1. Про основні засади забезпечення кібербезпеки України, Закон України від 05.10.2017, № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Конвенція про кіберзлочинність, Рада Європи, Конвенція, Міжнародний документ, від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

3. Кримінальний кодекс України, Кодекс України; Кодекс, Закон від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

УДК 004.93:351.74(477)

АНАЛІЗ СВІТОВИХ ПРАКТИК УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ПРИ ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Валентина ЯЩУК [1]
Олена ВОДНІЦЬКА [1]
Amiran SHARADZE [2]

[1]***Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.***
[2]***Batumi Shota Rustaveli State University, Batumi, Georgia.***

Abstract. *The theoretical and organizational and functional foundations of the implementation of global practices of cybersecurity management are considered. Modern approaches to cybersecurity management in modern realities are identified. Methodological approaches to the formation of the concept of cybersecurity management in ensuring information security of leading countries of the world are presented. The stages of solving the scientific and practical problem of cybersecurity management in ensuring information security of Ukraine are proposed based on the analysis of global practices.*

Keywords: *cybersecurity management, cybersecurity index, information security, cybersecurity strategy, critical infrastructure.*

Анотація. *Розглянуто теоретичні та організаційно-функціональні основи реалізації світових практик управління кібербезпекою. Визначено сучасні підходи до управління кібербезпекою у сучасних реаліях. Наведено методичні підходи до формування концепції управління кібербезпекою при забезпеченні інформаційної безпеки*

провідних держав світу. Запропоновано етапи вирішення науково-практичної проблеми управління кібербезпекою при забезпеченні інформаційної безпеки України на основі аналізу світових практик.

Ключові слова: *управління кібербезпекою, індекс кібербезпеки, інформаційна безпека, стратегія кібербезпеки, критична інфраструктура.*

Геополітичні реалії та стрімкий розвиток технологій сприяють зростанню кіберзагроз. Кібератаки стали повсякденним явищем і становлять серйозну загрозу для національної безпеки, економіки та суспільства в цілому. Україна, як країна, що активно розвивається в цифровому напрямку, є привабливою мішенню для кіберзлочинців. Кіберпростір перетворився на нове поле бою, де відбуваються гібридні війни. Російсько-українська війна продемонструвала масштаби використання кібератак як інструменту гібридної війни. Україна має розвинену критичну інфраструктуру (енергетика, транспорт, зв'язок), яка є життєво важливою для функціонування держави. Захист цієї інфраструктури від кібератак є одним із пріоритетних завдань. Україна активно рухається шляхом цифрової трансформації, що призводить до збільшення кількості підключених пристроїв та систем, що, в свою чергу, підвищує ризики кібератак.

Україна активно співпрацює з міжнародними організаціями в галузі кібербезпеки, що вимагає аналізу світових практик та адаптації їх до національних умов. Зростання кількості персональних даних, що зберігаються в електронному вигляді, вимагає вдосконалення заходів захисту від несанкціонованого доступу. Постійно змінюється законодавство в галузі кібербезпеки, що потребує аналізу та адаптації практик управління [1].

Національний індекс кібербезпеки (NCSI) – це глобальний індекс, який вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами. NCSI – це також база даних із загальнодоступними матеріалами та інструментарієм для розбудови потенціалу національної кібербезпеки. За останніми даними [2, 3] країни посідають такі місця за індексом NCSI: Естонія – 3 місце, Литва – 4 місце, Іспанія – 5 місце, Нідерланди – 10 місце, Сполучені Штати Америки – 14 місце, Велика Британія – 15 місце. Україна посідає за рейтингом NCSI 28 місце. NCSI розроблений і реалізується Фондом академії електронного врядування Естонії, натомість Глобальний індекс кібербезпеки (GCI) укладає Міжнародний союз електрозв'язку (МСЕ), він є ініціативою для зацікавлених сторін, спрямованою на підвищення обізнаності щодо кібербезпеки та вимірювання прихильності країн до кібербезпеки та її широкого застосування в різних галузях і секторах.

Рівень розвитку кожної країни аналізується за п'ятьма категоріями: правові заходи, технічні заходи, організаційні заходи, розбудова потенціалу та співробітництво. Відповідно до останнього GCI 2018 року, однакові бали за всіма п'ятьма категоріями набрали три країни [2, 3]: Велика Британія, Франція та Литва. За правовими та організаційними показниками всі набирають максимальний бал (0.200). Усі країни показують найнижчі (але все одно доволі

високі) бали в категорії співробітництва, при цьому високі, але не максимальні бали – в категоріях технічних заходів та розбудови потенціалу.

Велика Британія посідає перше місце з найвищими балами у двох категоріях – правові та організаційні заходи. Велика Британія має низку правових інструментів, що дають змогу боротися з кіберзлочинністю, зокрема Закон про зловживання комп'ютером. Національне агентство з питань злочинності успішно провело міжнародну операцію із закриття вебсайту, пов'язаного з 4 млн DDOS-атак у всьому світі. Франція вдруге посіла друге місце в Європі, при цьому набрала 100 відсотків за категоріями правових та організаційних заходів. Литва має найвищий бал як у правовій, так і в організаційній категорії. Закон Литви про кібербезпеку містить положення, що дозволяють компетентним органам вживати заходів проти загальнодоступної інфраструктури електронного зв'язку, яка бере участь у шкідливій онлайн-діяльності (*наприклад*, у ботнеті).

Державна інспекція захисту даних може публікувати інформацію про випадки, пов'язані з порушеннями персональних даних. Високі бали також набрали США (2 місце), Литва (4 місце), Естонія (5 місце), Іспанія (7 місце) Нідерланди (12 місце), Ізраїль (39 місце). Для порівняння, Україна посіла у рейтингу GCI 2018 року 54 місце. Саме ці сім провідних країн були обрані для огляду організаційних заходів, а також аналізу управління колективною кібербезпекою в ЄС.

Відтак, заслуговують на увагу законодавчі акти досліджуваних країн та інформація з офіційних сайтів органів, відповідальних за забезпечення кібербезпеки. Аналіз кращі практики управління кібербезпекою в країнах, що входять до десятки найуспішніших у сфері кібербезпеки і кіберзахисту в світі дозволяє виокремити такі структурні компоненти, як показники Національного індексу кібербезпеки (NCSI); огляд законодавчого забезпечення кібербезпеки, організаційна та інституційна складова, координація політики кібербезпеки, військова кібербезпека, запобігання критичним загрозам та кризам, державно-приватне партнерство та огляд суб'єктів, викликів і загроз у рамках національних стратегій.

Системи управління кібербезпекою в досліджуваних країнах, мають спільні особливості й кардинальні відмінності. Так, країни з системами прецедентного права (Велика Британія та США) використовують ризик-орієнтований підхід і на підставі оцінки ризиків та загроз готують стратегічні документи, плани їх реалізації, уточнюють повноваження інституцій відповідно до тих завдань, які ставить національна стратегія. Ще одна особливість цих країн – відсутність на перших етапах регулювання окремого закону про кібербезпеку. Велика роль відводиться самим суб'єктам кібербезпеки, їх свідомому підходу, а також системі стандартизації.

Так, у США NIST останнім часом здобув підтримку на законодавчому рівні. Найбільше від решти проаналізованих країн відрізняється підхід до кібербезпеки, застосовуваний в Ізраїлі. Ця країна постійно перебуває у ворожому

середовищі, має високий відсоток виробництва високотехнологічної продукції, що залежить від сталості цифрових послуг, і експортує програмне забезпечення, тож вважає забезпечення кібербезпеки одним із завдань оборони країни, використовує мілітаризований підхід і досить обмежено інформує про заходи, що будуть вживатися; крім того, активно залучає науковий потенціал і широко співпрацює з бізнесом, але залученість громадськості до формування політики низька. Близькими до України за організацією управління кібербезпекою є країни колишнього СРСР (Литва, Естонія), які ухвалили відповідні закони про кібербезпеку, чітко визначили повноваження основних суб'єктів кібербезпеки та встановили відповідальність за невиконання заходів.

У Литві стратегічні цілі та пріоритети політики кібербезпеки, а також заходи, необхідні для їх досягнення, визначає уряд, а не законодавчий орган чи Президент. Як найкращу практику регулювання в Україні можна адаптувати для застосування литовський закон про кібербезпеку, але з певними застереженнями, оскільки Литва як член ЄС визнає і без змін "переносить" Регламенти ЄС, що в Україні здійснити неможливо. Утім, нашій державі все одно слід імплементувати як Директиви, так і Регламенти ЄС у цій сфері. Країни "старої" Європи – Нідерланди та Іспанія (обидві за формою правління – монархії) – відзначаються досить цікавою організацією управління та взаємодії інституцій. І в Іспанії, і в Нідерландах до ухвалення рішень щодо формування та реалізації політики у сфері кібербезпеки залучені численні органи, а нормативно-правові акти вводяться в дію королівськими указами. У Нідерландах до системи забезпечення кібербезпеки включені також організації регіонального рівня [2, 3].

Слід зазначити, що в усіх країнах регулятори координують свою діяльність у сфері захисту персональних даних та у сфері кібербезпеки в частині інформування про інциденти, порушення цілісності систем, вироблення політики з метою уникнення дублювання повноважень тощо. Технічна частина системи захисту персональних даних регулюється законодавством у сфері кібербезпеки, а безпосередньо захист прав осіб – органом, що здійснює контроль у сфері захисту персональних даних. Окремо варто наголосити, що підхід європейських країн до забезпечення захисту об'єктів критичної інфраструктури уніфікований відповідно до Директиви NIS.

Висновки. Більшість європейських країн працюватимуть над імплементацією нового європейського законодавства у сфері кібербезпеки в частині поки що добровільної можливості для бізнесу засвідчувати, що його продукти відповідають стандартам кібербезпеки ЄС. Європейська Комісія регулярно проводитиме оцінку необхідності впровадження обов'язковості тієї чи іншої схеми сертифікації. Застосовувана схема сертифікації може визначати один або кілька рівнів забезпечення безпеки: базовий, значний або високий. На базовому рівні виробники ІКТ або постачальники послуг зможуть самі здійснювати оцінку відповідності. У разі значного чи високого рівня оцінювання здійснюватимуться національними органами з сертифікації кібербез-

пеки. Держави-члени ЄС розроблять правила щодо покарань за порушення Основ та схем сертифікації кібербезпеки ЄС та надаватимуть ширші компетенції органам, відповідальним за кібербезпеку, для забезпечення співпраці й застосування рекомендацій ENISA.

Інформаційні джерела

1. Ящук В. І. Роль та місце стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави. Moderní aspekty vědy: XLII. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. str. 364. pp. 259–286.

2. ENISA. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ national-cybersecurity-strategies-interactive-map.

3. Кращі практики управління кібербезпекою. Оглядовий звіт. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf

4. Ящук В. І. Методика забезпечення безпеки інформаційних систем та реагування на кіберінциденти кібербезпековими центрами. Scientific Collection “InterConf+”, 45(201): with the Proceedings of the 8thInternational Scientific and Practical Conference “International Scientific Discussion: Problems, Tasks and Prospects” (May19–20, 2024; Brighton, United Kingdom)/ comp. by LLC SPC “InterConf”.Brighton: A.C.M. Webb Publishing Co Ltd., 2024. 678 p. pp. 632–641.

УДК 007:316.77

МОДЕЛЬ ПОВЕДІНКИ “АГЕНТІВ” ВОЄННОЇ КОМУНІКАЦІЇ: ФОРМАЛЬНО-СИНТАКСИЧНА ІЄРАРХІЯ

Юлія ДЕМ’ЯНЧУК
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The article explores the model of behavior of “agents” of military communication in texts of official-business style of speech. Formal-syntactic hierarchies and linguistic tools that construct communicative models are analyzed. Particular attention is paid to war-related collocations and their role in the strategic management of the content of military rhetoric.*

Keywords: *agents of military communication, war-related collocations, syntactic models, international politics, military rhetoric.*

Анотація. *Стаття досліджує модель поведінки “агентів” воєнної комунікації у текстах офіційно-ділового стилю мовлення. Аналізуються формально-синтаксичні ієрархії та лінгвістичні інструменти, які конструюють комунікативні моделі. Окрему увагу приділено war-related collocations та їхній ролі у стратегічному управлінні змістом воєнної риторики.*

Ключові слова: *агенти воєнної комунікації, war-related collocations, синтаксичні моделі, міжнародна політика, воєнна риторика.*

"Агенти воєнної комунікації" в тексті офіційно-ділового стилю мовлення у нашому дослідженні це – фізичні особи (політик, депутат, консул, посол та інші), а також інституції (органи державної влади, міжнародні парламентські організації, загальнополітичні організації), що виконують роль посередників у висвітленні публічних заяв, дипломатичних протоколів, нормативно-правових актів. Мовні засоби вербалізації воєнної комунікації, представлені *war-related collocations,* референти яких конструюють комунікативні моделі.

Розмежування формально-синтаксичної ієрархії й моделей поведінки агентів воєнної комунікації в системі різнорівневих синтаксичних структур визначає архітектоніку комунікативного акту в тексті офіційно-ділового стилю. Випрацювання *war-related collocations* у воєнній комунікації відбувається на декількох рівнях:

1) базовому – на цьому рівні колокації формують основу комунікативного акту;

2) дискурсивному – у площині цього виміру, колокації є когнітивно-афективними елементами дискурсу, смисловими сегментами, що підтримують визначену риторику;

3) метарівні – у межах визначеного рівня, колокації слугують лінгвістичними моделями стратегічного управління, що оприявнюють комунікативну мету, впливають на спосіб подання інформації.

Нижче описано механізм застосування моделі поведінки агентів воєнної комунікації:

Russia must be held accountable for these horrible acts. This is a terrible crime, inflicting unimaginable suffering," said Šuica. "Investing in children is an investment in Ukrainians' future, in Europe's future and in a safer world. So, it is an investment in humanity [EU NEIGHBOURSEAST 2024].

13 березня 2024 року Єврокомісія відзвітувала перед Європарламентом про свою діяльність у зв'язку з примусовою депортацією Росією українських дітей. У своїй промові від імені Верховного представника ЄС Жозепа Борреля (Josep Borrell) віце-президент Європейської комісії з питань демократії та демографії Дубравка Шуїца (Dubravka Šuica) заявила, що ЄС повністю підтримує низку різних ініціатив. Зокрема, Росія має відповісти *(Russia must be held accountable)* за жахливі дії *(horrible acts)* в Україні. За словами Шуїци, ЄС докладає всіх необхідних зусиль, щоб винні у жахливому злочині *(terrible crime)* незаконної депортації чи передачі українських дітей були притягнуті до відповідальності.

Метафори інвестиція в дітей *(investing in children),* інвестиція в майбутнє українців *(investment in Ukrainians' future),* інвестиція у майбутнє Європи *(investment in Europe's future),* інвестиція в безпечніший світ *(investment safer world)* та інвестиція в людство *(investment in humanity)* підсилюють ініціативу сімнадцяти держав-членів, що розпочали розслідування міжнародних злочинів, скоєних в Україні, і Європейський Союз підтримує ці національні розслідування шляхом зміцнення судової співпраці через Євроюст. Семан-

тизація поняття *terrible crime* (жахливий злочин) здійснюється на протиставленні safer world *(безпечніший світ),* що засвідчує об'єднання зусиль української влади, іноземних урядів та міжнародних організацій з метою повернення дітей до України та превенцію подібних злочинів.

Представлена в цьому текстовому фрагменті конструкція *Russia must be held accountable* детермінує модель поведінки "агента воєнної комунікації" – представниці ЄС Дубравки Шуїци. Формально-синтаксичний сегмент демонструє структуру висловлювання, спосіб вираження імперативних вимог в контексті міжнародної політики (рис. 1).

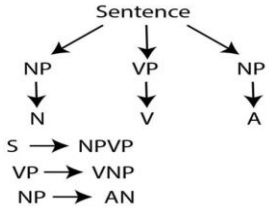


Рисунок 1 – Дерево складових сегмента тексту

Лінгвістична особливість формально-синтаксичного сегменту полягає в тому, що він створений з іменника *(Russia)* в імперативній функції, що підтверджує фінальна конструкція – Russia must be held. Модус владних приписів передає невідкладність і обов'язковість протидіяти Росії, шляхом зміцнення судової співпраці через Євроюст (європейське агентство, що співпрацює з судовими та поліцейськими органами країн-членів ЄС). Дисперсний елемент сегмента тексту *accountable* втілює стратегію впливу на міжнародну спільноту, підкреслює необхідність реагувати на агресію Росії згідно міжнародних стандартів ЄС.

Модель поведінки агента воєнної комунікації утілює синтаксична конструкція *Russia must pay for these appalling violations,* яка виводить на поверхню дискусії необхідність покарання країни-агресора. Ієрархію міжкомпонентних зв'язків у площині синтаксичної конструкції ілюстровано нижче (рис. 2):

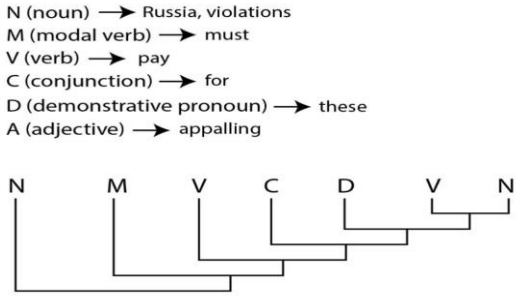


Рисунок 2 – Ієрархія зв'язків в синтаксичній конструкції Russia must pay for these appalling violations

Бінарна діада Russia=violations, відповідним чином констатує вплив на реципієнтів відображає модель поведінки референтів комунікативного акту; розширює палітру соціокультурного представлення правди і справедливості. Певною мірою, кореляційний зв'язок можна вважати причинно-наслідковим, стосовно суб'єкта та його дій, оскільки ієрархічні зв'язки в синтаксичній конструкції виформовують стійку асоціацію (жорстокий) в свідомості реципієнтів.

В Україні з початку 2023 року функціонує Офіс Міжнародного кримінального суду. Співпраця між Україною та Міжнародним кримінального судом має за мету забезпечити ефективне міжнародне кримінальне правосуддя.

For more than a year now, Russia's war of aggression has disregarded the foundations of our international rules-based order and destroyed the lives of many. It is against this background that the ICC has stepped up its efforts in investigating the international crimes that are being committed on Ukrainian soil on a daily basis. It is clear that when it comes to preventing impunity for the most serious crimes committed during this war, the International Criminal Court remains the key international actor to investigate and prosecute the perpetrators...<> And we must support Ukraine and the ICC in achieving these goals [Khan 2023].

Модель поведінки прокурора Міжнародного кримінального суду сигналізує про підтримку України. Синтаксичні зв'язки у реченні *And we must support Ukraine and the ICC in achieving these goals,* орієнтовані на дифузію широкого поняттєвого значення. Вербальне оформлення моделі поведінки у воєнній комунікації може мати різну протяжність. Формально-синтаксична схема відображає шість відрізків мовлення, які орієнтовані на дескриптивний потенціал їхньої семантики (рис. 3).

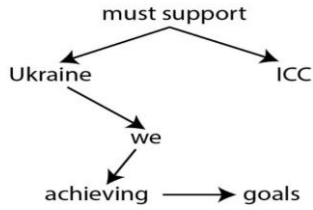


Рисунок 3 – Схема речення граматики залежностей

Візуалізація граматики залежностей у цьому випадку відображає структуру синтаксичних зв'язків між ключовими елементами речення. Вона демонструє, як кожен компонент речення вказує на підрядний зв'язок та аппозитивні відношення. На нерозривну єдність "агента воєнної комунікації" й воєнно-політичного цілого вказує розгортання відповідної підтримки з боку Європейського союзу, що пов'язане з систематичним посиленням політичної, економічної та військової допомоги Україні. З огляду на представлені особливості, Європейська Комісія надала понад 10 мільйонів євро на підт-

римку роботи Міжнародного кримінального суду щодо розслідувань воєнних злочинів в Україні. З жовтня 2023 року в Києві функціонує Представництво Міжнародного кримінального суду.

Висновки. Отже, модель поведінки "агентів воєнної комунікації" в текстах офіційно-ділового стилю демонструє, як мовні інструменти слугують механізмом інституційного впливу, підсилюючи легітимність дій і рішень на геополітичній авансцені.

Інформаційні джерела

1. EU NEIGHBOURSEAST. (2024) Investment in humanity: Russia must be held accountable for deportations of Ukrainian children, says EU. URL: https://euneighbourseast.eu/news/latest-news/investment-in-humanity-russia-must-be-held-accountable-for-deportations-of-ukrainian-children-says-eu/

2. Khan A. (2023) Opening remarks by Commissioner Reynders at the Justice Ministers Conference on Support to the International Criminal Court and its Investigations into the Situation in Ukraine. European Commission. URL: https://ec.europa.eu/commission/ presscorner/detail/en/speech_23_1786

УДК 342.951:004.056.5

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙНИ

Андрій ХАРЧУК
Андрій ХАРЧУК

Інститут післядипломної освіти Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The article analyzes the legal support for information security in Ukraine under martial law. Key regulatory legal acts are considered, in particular, the "Information Security Doctrine of Ukraine" and decisions of the National Security and Defense Council. The emphasis is on the protection of the state information system, counteraction to disinformation and adaptation of legislation to war conditions.*

Keywords: *information security, martial law, disinformation, legal support, National Security and Defense Council, Information Security Doctrine of Ukraine, legislation.*

Анотація. *Стаття аналізує правове забезпечення інформаційної безпе-ки України в умовах воєнного стану. Розглядаються ключові нормативно-правові акти, зокрема "Доктрина інформаційної безпеки України" та рішення РНБО. Акцентовано увагу на за-хисті державної інформаційної системи, протидії дезінформації та адаптації законодавства до умов війни.*

Ключові слова: *інформаційна безпека, воєнний стан, дезінформація, правове забезпечення, РНБО, Доктрина інформаційної безпеки України, законодавство.*

У сучасних умовах правового режиму воєнного стану питання забезпечення інформаційної безпеки в Україні відіграє роль інструменту протистояння. Це фактично зброя, за допомогою якої можуть вигравати війни без жодного пострілу.

Слід звернути увагу на те, що в цих умовах цілий комплекс інформації розрахований на маніпулювання громадською думкою та свідомістю людини. Така інформація подається за допомогою фізіологічних і психологічних засобів її сприйняття.

Українське законодавство у сфері інформаційної безпеки визначає основоположні принципи та механізми забезпечення інформаційної безпеки, зокрема в Конституції України, законах України, рішеннях РНБО та інших нормативно-правових актах.

Цілком справедливо вважається, що інформаційна безпека передбачає:

– належний рівень інформаційної культури, тобто підготовку особистості, що забезпечує захист і реалізацію її життєво важливих інтересів незалежно від наявності інформаційних загроз;

– здатність держави створити умови для гармонійного розвитку та інформаційних потреб особи;

– забезпечення, розвиток і використання інформаційного середовища в інтересах особи;

– захист від різноманітних інформаційних загроз [5].

Відповідно, сьогодні на передньому плані стоять завдання щодо захисту інформаційної системи нашої держави від несанкціонованого інформаційного впливу та захисту громадян від дезінформації, шахрайства, спотвореної та викривленої інформації.

Інформаційна безпека включає не лише нормативну складову, але й діяльність органів, що її забезпечують. З цією метою Указом Президента України від 25.02.2017 року була затверджена “Доктрина інформаційної безпеки України” [1].

У сучасних умовах війни, 18.03.2022 року, РНБО ухвалила рішення щодо реалізації єдиної інформаційної політики в умовах воєнного стану. У ньому визначено, що реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки. безпеки [2].

Більш того, в Україні діє Центр протидії дезінформації при РНБО України, на сайті якого можна ознайомитися з актуальною інформацією та подіями в цій сфері.

Норми Кримінального кодексу структуровано визначають види злочинів у інформаційній сфері та відповідальність за їх вчинення [4].

В цілому нормативно-правові акти в сфері інформаційної безпеки сформовані. Проте існує потреба в унормуванні суспільних відносин в умовах війни. Зокрема, ми бачимо внесення змін до нормативно-правових актів, що

регулюють питання забезпечення реальних механізмів юридичного захисту порушених прав громадян нашої держави в інформаційному просторі.

Таким прикладом є рішення Ради національної безпеки і оборони України "Про нейтралізацію загроз інформаційній безпеці держави" від 19 березня 2022 року №151/2022 [3].

Висновки. Отже, зміни, які відбуваються в законодавчій базі України щодо забезпечення інформаційної безпеки в умовах війни, є вкрай важливими для розвитку та забезпечення інформаційного простору держави.

Інформаційні джерела

1. Указ Президента України від 25.02.2017 р. "Доктрина інформаційної безпеки України".

2. Рішення РНБО України від 18.03.2022 р. щодо реалізації єдиної інформаційної політики в умовах воєнного стану.

3. Рішення РНБО України від 19.03.2022 р. №151/2022 "Про нейтралізацію загроз інформаційній безпеці держави".

4. Кримінальний кодекс України/ Редакція від 13.04.2022. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

5. Інформаційна безпека. Підручник. Під ред. В. В. Остухова. К.: Видавництво Ліра-К, 2021.

УДК 004.056.5

РОЗСЛІДУВАННЯ КІБЕРАТАК У ВОЄННИХ УМОВАХ

Валерій БУНДУС
Василь ЛУЧИК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract*. The article examines key aspects of investigating cyberattacks in military settings, which is an important component of national security. Cyberspace has become one of the main battlefields of modern warfare with attacks aimed at destabilizing critical systems, moral damage and compromising data. The main stages of using monitoring systems to investigate attacks, collect evidence, analyze vulnerabilities and sources of threats are discussed. Special attention is paid to the connections between cyberattacks and physical attacks, which require close coordination between agencies. The need for international cooperation to effectively counter threats is outlined. This work emphasizes the importance of technical expertise and comprehensive approaches to ensuring the country's cyber defense in the complex conditions of hybrid warfare.*

Keywords. *Cyber security, cyber threats, national security, monitoring, investigation, hybrid war.*

Анотація. *У статті розглядаються ключові аспекти розслідування кібератак у військових умовах, що є важливою складовою національної безпеки. Кіберпростір став одним із головних полів бою сучасної війни з атаками, спрямованими на дестабілізацію критично важливих систем, моральну шкоду та компрометацію даних. Розглянуто основні етапи використання систем моніторингу для розслідування атак, збору доказів, аналізу вразливостей і джерел загроз. Особливу увагу приділено зв'язкам між кібератаками та фізичними атаками, які вимагають тісної координації між відомствами. Окреслено необхідність міжнародної співпраці для ефективної протидії загрозам. Ця робота підкреслює важливість технічної експертизи та комплексних підходів до забезпечення кіберзахисту країни в складних умовах гібридної війни.*

Ключові слова. *Кібербезпека, кіберзагрози, національна безпека, моніторинг, розслідування, гібридна війна.*

Розслідування кібератак у воєнних умовах є важливим аспектом забезпечення національної безпеки, адже кіберпростір перетворився на одне з ключових полів сучасної війни. У контексті військових конфліктів кібератаки стають складними і добре організованими, їхньою метою є не лише знищення інфраструктури, але й підрив морального духу населення, компрометація даних та дестабілізація роботи критичних систем. Такі атаки часто спрямовані на енергомережі, фінансові установи, транспортні системи та державні органи, що робить їх надзвичайно небезпечними в умовах війни.

Одним із перших кроків у розслідуванні є виявлення самого факту атаки. Для цього використовуються сучасні системи моніторингу, які дозволяють аналізувати потоки даних, журнали подій та поведінку мережевих систем. Виявлення аномалій, таких як незвичний обсяг трафіку чи спроби доступу до захищених даних, може вказувати на потенційну атаку. Далі розпочинається етап збору доказів: аналізується мережевий трафік, зразки шкідливого програмного забезпечення, дані з журналів серверів та систем [1].

Ключовим етапом є аналіз атаки, під час якого визначаються вектори проникнення та вразливості, використані зловмисниками. *Наприклад*, атака могла бути здійснена через фішингову кампанію, використання експлойтів чи компрометацію облікових записів. Важливим завданням цього етапу є також ідентифікація джерела атаки. Це складний процес, адже зловмисники часто приховують свої сліди, використовуючи ботнети, проксі-сервери чи сервери у третіх країнах. Для визначення реальних винуватців залучаються інструменти трасування, аналіз зразків шкідливого коду та розвіддані про вже відомі кіберзагрози [2].

Особливістю розслідування кібератак у воєнний час є їхній зв'язок із фізичними атаками. *Наприклад*, атака на енергомережу може супроводжуватися реальним ударом по об'єктах енергетичної інфраструктури. Це вимагає координації між різними відомствами, включаючи силові структури, розвідку та фахівців з кібербезпеки. Також розслідування ускладнюється обмеже-

ними ресурсами, адже у воєнних умовах доступ до спеціалістів та обладнання може бути суттєво обмеженим.

На завершальному етапі оцінюються збитки від атаки та впроваджуються заходи для запобігання повторним інцидентам. Важливо відновити роботу систем, забезпечити резервне копіювання критичних даних та виявити слабкі місця у захисті. Міжнародне співробітництво відіграє ключову роль у боротьбі з кібератаками, адже обмін інформацією про загрози та методи реагування допомагає швидше нейтралізувати атаки та ідентифікувати їхні джерела.

Таким чином, розслідування кібератак у воєнних умовах є складним, але життєво необхідним процесом, який вимагає поєднання технічної експертизи, злагодженої роботи різних відомств та міжнародної співпраці. Це дозволяє не лише захистити критичні системи, але й зберегти стійкість держави в умовах гібридної війни.

Інформаційні джерела

1. Кібербезпека під час повномасштабного вторгнення: неочікувані принципи кібергігієни – Lviv IT Cluster. Lviv IT Cluster. URL: https://itcluster.lviv.ua/itid/kiberbezpeka-pid-chas-povnomasshtabnogo-vtorgnennya-neochikuvani-prynczypy-kibergigiyeny/ (дата звернення: 16.11.2024).

2. Кібертероризм в сучасному світі: як завадити фішингу, вірусам та іншим загрозам. URL: https://dou.ua/forums/topic/49184/ (дата звернення: 16.11.2024).

Напрям 2

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В ПІДРОЗДІЛАХ МВС УКРАЇНИ

УДК 621.39

ПРОТИДІЯ ВИТОКУ ІНФОРМАЦІЇ З ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ В ПІДРОЗДІЛАХ МВС УКРАЇНИ

Роман БОРМАТОВ

Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *Counteracting technical information leakage channels in the units of the Ministry of Internal Affairs of Ukraine is crucial for ensuring national information security. This article examines the main types of technical information leakage channels, including radio, electrical, acoustic, and optical channels, along with methods for their detection and neutralization. A comprehensive set of organizational, technical, and software measures is presented, such as the use of white noise generators, shielding materials, modern cryptographic algorithms, and monitoring systems. The focus is on a multilayered approach to building an information protection system integrated with other aspects of security, including cybersecurity. The importance of regularly updating protection measures, training personnel, and monitoring threats for effectively preventing information leaks is highlighted.*

Keywords: *technical leakage channels, information security, acoustic protection, electromagnetic radiation, cryptography, information protection, Ministry of Internal Affairs of Ukraine.*

Анотація. *Протидія технічним каналам витоку інформації в підрозділах Міністерства внутрішніх справ України є критично важливою для забезпечення національної інформаційної безпеки. У статті розглянуто основні типи технічних каналів витоку інформації, зокрема радіоканали, електричні, акустичні та оптичні, а також методи їх виявлення й нейтралізації. Представлено комплекс організаційних, технічних і програмних заходів, таких як застосування генераторів білого шуму, екранізуючих матеріалів, сучасних криптографічних алгоритмів і систем моніторингу. Акцент зроблено на багаторівневому підході до побудови системи захисту інформації, інтегрованій з іншими аспектами безпеки, включаючи кіберзахист. Висвітлено важливість регулярного оновлення засобів захисту, навчання персоналу й моніторингу загроз для ефективної протидії витокам інформації.*

Ключові слова: *технічні канали витоку, інформаційна безпека, акустичний захист, електромагнітне випромінювання, криптографія, захист інформації, МВС України.*

Вступ. Протидія технічним каналам витоку інформації в підрозділах Міністерства внутрішніх справ України є важливою складовою забезпечення інформаційної безпеки. У сучасних умовах, коли інформація є стратегічним ресурсом, її витік може призвести до значних негативних наслідків, включаючи підрив державної безпеки, дискредитацію органів влади, втрату довіри громадян і компрометацію оперативно-службової діяльності. У цьому контексті ключовим завданням стає мінімізація ризиків несанкціонованого доступу до інформації та запобігання її витоку через технічні канали.

Основна частина. Під технічним каналом витоку інформації розуміють сукупність об'єкта розвідки, технічного засобу розвідки (ТЗР), за допомогою якого збирається інформація про об'єкт, і фізичного середовища, де розповсюджується інформаційний сигнал.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх розповсюдження і способів перехоплення ТЗР більш детально технічні канали витоку інформації можна поділити на:

– радіоканали (електромагнітне випромінювання радіодіапазону);

– електричні (засоби провідникового зв'язку та різні струмопровідні комунікації) можуть виникати через випромінювання, що створюється електронними пристроями, тоді як вібраційний витік можливий через аналіз вібрацій конструкцій, викликаних, *наприклад*, друкарськими пристроями);

– акустичні (розповсюдження звукових коливань) можуть відбуватися через перехоплення звукових сигналів за допомогою мікрофонів, диктофонів або направлених акустичних приймачів;

– оптичні (електромагнітне випромінювання в інфрачервоній і ультрафіолетовій частини спектру) стає можливим через несанкціоноване спостереження, зокрема, із використанням відеокамер чи оптичних приладів [1, с. 73].

У підрозділах МВС для протидії технічним каналам витоку інформації застосовують комплекс організаційних та технічних заходів. Організаційні заходи включають створення режиму обмеженого доступу до приміщень, де обробляється конфіденційна інформація, впровадження суворих правил щодо використання технічних засобів і проведення регулярного навчання співробітників. Забезпечення фізичного контролю над доступом до приміщень дозволяє мінімізувати ризики встановлення несанкціонованих пристроїв зйому інформації.

Технічні заходи протидії витоку інформації включають використання спеціалізованого обладнання для виявлення і нейтралізації пристроїв перехоплення. Для запобігання акустичним витокам застосовують генератори білого шуму, які створюють звукові перешкоди, що ускладнюють аналіз записаного звуку. Для захисту від електромагнітного випромінювання використовуються екрановані приміщення або спеціальні екрани для пристроїв, що зменшують рівень випромінювання. Для запобігання оптичним витокам застосовують захисні плівки на вікнах, які перешкоджають зчитуванню

інформації через оптичні прилади. Виявлення несанкціонованих пристроїв запису забезпечується шляхом періодичного радіомоніторингу та перевірки приміщень на наявність прихованих пристроїв.

Методи протидії технічним каналам витоку інформації.

Захист від акустичних витоків**:**

– Генератори білого шуму генерують широкосмугові перешкоди, що ускладнюють прослуховування акустичної інформації за допомогою мікрофонів.

– Для ізоляції акустичних хвиль приміщення можуть бути оснащені звукопоглинальними матеріалами (спеціальні панелі, обшивка стін).

– Встановлення спеціальних ущільнювачів на дверях, що запобігають проходженню звукових хвиль [2, с. 11].

Ключову роль у протидії витоку інформації відіграє моніторинг технічних засобів і регулярне тестування системи захисту. Використання сучасних технологій, таких як системи активного виявлення електромагнітних полів і аналізаторів акустичних сигналів, дозволяє підвищити ефективність заходів захисту. Важливим є також регулярне оновлення методик і засобів протидії у відповідь на розвиток технічних засобів перехоплення.

Захист від електромагнітних випромінювань**:**

– Використання екранів із металевих матеріалів для обладнання та приміщень, які знижують рівень електромагнітного випромінювання.

– Інсталяція фільтрів на мережі електроживлення для нейтралізації випромінювання.

Криптографічний захист:

– Використання сучасних алгоритмів шифрування для захисту даних, що передаються, *наприклад*, AES-256.

– Впровадження інфраструктури відкритих ключів (PKI) для забезпечення конфіденційності обміну даними між працівниками [2, с. 13].

Не менш важливою є інтеграція системи захисту інформації з іншими заходами безпеки в МВС, включаючи кібербезпеку та захист даних від несанкціонованого доступу. Синергія між різними рівнями захисту створює багаторівневий бар’єр проти витоків інформації.

Оновлення програмного забезпечення:

– Регулярна перевірка оновлень операційних систем і програм для усунення вразливостей.

– Використання антивірусного програмного забезпечення з актуальними базами даних.

Ці заходи формують багаторівневу систему захисту, яка забезпечує безпеку інформації у підрозділах МВС. Якщо потрібно ще більше розкрити окремі аспекти, дайте знати!

Висновки. Протидія технічним каналам витоку інформації в підрозділах МВС України є важливою складовою забезпечення інформаційної безпеки,

що спрямована на захист стратегічних даних і запобігання їх несанкціонованому розголошенню. Використання комплексних організаційних, технічних і програмних заходів дозволяє значно зменшити ризики витоку інформації. Особлива увага приділяється захисту від акустичних, електромагнітних, оптичних і інших технічних загроз. Ефективна реалізація цих заходів потребує постійного моніторингу сучасних загроз, вдосконалення засобів захисту, навчання персоналу та інтеграції різних рівнів інформаційної безпеки, включаючи кіберзахист. Системний підхід до побудови багаторівневого бар'єра проти витоків забезпечує не лише збереження конфіденційності, але й підвищує ефективність оперативно-службової діяльності МВС, що має безпосередній вплив на національну безпеку держави.

Інформаційні джерела

1. Рибальский О. В., Смаглюк В. М., Хахановський В. Г. Основи інформаційної безпеки : підручник. Київ, 2011. 245 с.

2. Львівський державний університет внутрішніх справ. Інформаційна безпека у телекомунікаційній мережі НПУ: кейс заняття. Львів, 2022. 19 с.

УДК 004.056

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В ОРГАНАХ ТА ПІДРОЗДІЛАХ ДСНС УКРАЇНИ

Володимир ПИЛИПЕНКО
Олександр ТИМЧИШИН
Назарій ФЕДЕЦЬ

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *Technical protection of information in the units of the State Emergency Service of Ukraine is an important component of ensuring the reliability of processing and protecting critical systems from cyber threats. The main principles, protection methods and recommendations for improving cybersecurity in the bodies and units of the State Emergency Service of Ukraine are considered. Ensuring information security is the key to effective activity in emergency conditions. Investigation of cases of violations of norms and requirements on information security issues that pose a threat to the confidentiality, integrity and availability of information.*

Keywords*: technical protection, SES of Ukraine, information security, cyber threats. однією з найважливіших сфер, а особливо в державному секторі.*

Анотація. *Технічний захист інформації у підрозділах ДСНС України є важливою складовою забезпечення надійності обробки та захист критично важливих си-*

стем від кіберзагроз. Розглянуто основні принципи, методи захисту та рекомендації щодо вдосконалення кібербезпеки в органах та підрозділах ДСНС України. Забезпечення інформаційної безпеки є запорукою ефективної діяльності в надзвичайних умовах. Розслідування випадків порушення норм та вимог з питань ТЗІ, що створюють загрозу конфіденційності, цілісності та доступності інформації.

***Ключові слова**: технічний захист, ДСНС України, інформаційна безпека, кіберзагрози.*

У сучасних світових реаліях та з початком повномасштабної війни на території України, забезпечення кібербезпеки державного сектору стало одним з пріорітетним завданням, яке постало перед державою і зокрема перед Державною службою України з надзвичайних ситуацій (далі – ДСНС України). Для забезпечення кібербезпеки в інформаційних системах ДСНС України, визначають основні цілі та ризики, щоб встановити пріоритет їх значущості щодо зниження ризиків та зуміти реалізувати механізми управління ними на всіх критичних об'єктах інформаційної інфраструктури. Оскільки, інформації обробляється дуже багато, пов'язаної з управлінням наявних сил та засобів, які ліквідовують наслідки надзвичайних ситуацій, залучені до евакуації населення, а також зберігають конфіденційну інформацію співробітників та громадян. Якщо цю інформацію не захистити як слід це призведе до витоку персональних даних та інформації з обмеженим доступом, а використання її в корисливих цілях зловмисників буде загрожувати безпеці як працівників ДСНС України, так і державі в цілому. В умовах війни це дуже гостре питання, адже ворог здійснює сотні масованих кібератак кожного дня на ресурси ДСНС України.

Отож головні загрози захисту інформації:

– захист від кіберзлочинності;

– кібератаки на системи управління;

– захист від несанкціонованого доступу до інформації;

– забезпечення надійного функціоналу систем в умовах війни.

Основні кіберзагрози, які фіксують в інформаційних системах ДСНС України відбуваються за допомогою шкідливого програмного забезпечення, а саме:

– класичні комп'ютерні віруси ("троянський кінь", мережеві черв'яки);

– спеціальними засобами (експлойти, генератори ключів).

Тож розглянемо системи, які борються з кібератаками. Одною з якої є система контролю та управління доступу (СКУД), яка являє собою поєднання технічних та програмних засобів. Вона забезпечує доступ до об'єктів, інформацію про події та ідентифікацію суб'єкта. Також є системи моніторингу кіберзагроз. Апаратні та програмні мережеві екрани (фаєрволи), які запобігають несанкціонованому доступу до мережі ДСНС України.

Державні платформи кіберзахисту така як національна платформа "Державний центр кіберзахисту Держспецзв'язку" допомагає відстежувати та реагувати на загрози в державних органах та критично важливих структу-

рах не виняток й внутрішні інформаційні системи ДСНС України, які використовує для обміну даними про виникнення надзвичайних ситуацій. Протидія кіберзагрозам в ДСНС України включає регулярне оновлення антивірусних баз, виконання перевірок щодо відповідності нормативним вимогам з кібербезпеки. Окрім того, важливо здійснювати контроль за функціонуванням служб захисту інформації та кібербезпеки в інформаційно-телекомунікаційних системах, що знаходяться на об'єктах органів та підрозділів ДСНС України. Важливим аспектом є регулярне оновлення антивірусного програмного забезпечення (*наприклад*, антивірус Zillya!) для захищених комп'ютерів, що здійснюється кожного тижня, що є необхідною мірою для забезпечення захисту від кіберзагроз.

Правові основи технічного захисту інформації в ДСНС України

Технічний захист інформації в Україні коригується Положенням про технічний захист інформації, затвердженим Указом Президента України від 27 вересня 1999 року № 1229. У цьому Положенні виявити основи, принципи та порядок захисту інформації, яка підлягає захисту відповідно до законодавства, в установах та організаціях, що належать до сфери ДСНС України. Важливою складовою є організація відповідальних структур для виконання вимог технічного захисту та кібербезпеки. Організація технічного захисту інформації та відповідальність за його стан в апараті ДСНС України та Установах полягає на керівників. До об'єктів технічного захисту належить інформація, вимога щодо захисту якої встановлена законом. До об'єктів захисту ІТС, крім того, відноситься програмне забезпечення, що призначене для обробки цієї інформації. Організаційна структура та завдання комісії з технічного захисту інформації. Комісія з питань технічного захисту інформації в ДСНС України призначається наказом керівника організації. Очільником комісії є заступник керівника установи, а його заступником – керівник підрозділу зв'язку та інформатизації. Це забезпечує ефективне управління та координацію дій, спрямованих на технічний захист інформації. Оскільки захист інформації є пріоритетним завданням, головним завданням комісії є розробка заходів для забезпечення безпеки інформації, що циркулює в системах установи.

Основні завдання і функції у сфері технічного захисту інформації

Захист інформації: Основним завданням є організація захисту інформаційних ресурсів і забезпечення технічної безпеки на всіх рівнях управління. Це включає як захист від зовнішніх кіберзагроз, так і внутрішній захист від витоків конфіденційної інформації.

Контроль за виконанням вимог технічного захисту інформації та кібербезпеки є важливою частиною роботи підрозділів служб захисту інформації. Проводяться перевірки, що включають перевірку стану виконання вимог законодавства з питань захисту інформації та кібербезпеки, а також перевірки на наявні кібер загрози на робочих машинах.

Забезпечення захисту інформації та оновлення токенів

Щорічно здійснюється оновлення токенів доступу до інформаційних систем, що є частиною заходів з технічного захисту. Це забезпечує безпеку та правильне функціонування систем доступу до інформації, що є критично важливою для захисту державних ресурсів.

Запити до Держспецзв'язку та взаємодія з іншими органами

Для забезпечення належного рівня кібербезпеки та захисту інформації в установах ДСНС кожного року надаються запити до Держспецзв'язку щодо розташування іноземних представництв поблизу установ Головних управлінь ДСНС України. Це дозволяє вчасно виявляти потенційні загрози та вжити необхідних заходів для забезпечення безпеки. Розслідування порушень та заходи для попередження. Участь в розслідуванні порушень вимог щодо технічного захисту інформації та кібербезпеки. В разі виявлення порушень вживаються заходи для усунення ризиків та запобігання подібним ситуаціям у майбутньому.

Висновки. У сучасних умовах забезпечення інформаційної безпеки є не лише технічним завданням, але й складовою стратегічного управління, що дозволяє ДСНС України ефективно функціонувати в надзвичайних умовах і гарантувати захист громадян та держави. Для надійного захисту інформаційних ресурсів потрібний належний контроль, що включає регулярне оновлення систем захисту інформації. *Наприклад*, системи моніторингу, які використовують штучний інтелект, який останнім часом сильно розвинувся, яким можна аналізувати загрози різних типів. Постійне вдосконалення нормативно-правових актів. Співпраця з партнерами інших країн для обміну досвідом, інформацією та залучання технічної допомоги та фахівців в галузі забезпечення кібербезпеки. Також важливе проведення регулярних навчань серед працівників щодо правильного використання інформаційних систем та сервісів в умовах воєнного стану Проводити різні контрольовані атаки на інформаційні системи, щоб бачити де є вразливості та вдосконалювати системи захисту.

Інформаційні джерела

1. Стратегія кібербезпеки України. URL: https:// zakon.rada.gov.ua/laws/show/447/2021#Text

2. Стандарти ISO/IEC управління інформаційною безпекою. URL: https:// studfile.net/preview/5367198/page:3/

3. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/uk.

4. Наказ ДСНС 01.10.2020 №533 "Положення з організації заходів забезпечення кібербезпеки ДСНС"

Напрям 3

БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

УДК 004.056.53

AI IN ACTION: DEFENDING AGAINST EVOLVING CYBER THREATS

Kostiantyn SAVCHUK
Lviv Polytechnic National University, Lviv, Ukraine.

Анотація. *Штучний інтелект змінює кібербезпеку, покращуючи виявлення загроз, прогнозування та автоматичні відповіді для боротьби зі складними атаками, такими як програми-вимагачі та фішинг. Пропонуючи швидкість і точність, він створює такі проблеми, як агресивні атаки та проблеми з конфіденційністю. Етичний ШІ, людський нагляд і глобальна співпраця є важливими для ефективного та відповідального розгортання.*

Ключові слова*: кібербезпека, штучний інтелект, програми-вимагачі, фішинг, виявлення аномалій, складні цільові атаки, атаки на ланцюг поставок.*

Abstract. *AI is transforming cybersecurity by enhancing threat detection, prediction, and automated responses to tackle advanced attacks like ransomware and phishing. While offering speed and accuracy, it raises challenges like adversarial attacks and privacy concerns. Ethical AI, human oversight, and global collaboration are essential for effective and responsible deployment.*

Keywords*: cybersecurity, Artificial Intelligence (AI), ransomware, phishing, anomaly detection, Advanced Persistent Threats (APTs), supply chain attacks.*

In our increasingly digital world, cybersecurity isn't just a tech issue−it's a critical concern for everyone. Cyber-attacks have become more sophisticated, and traditional security measures often struggle to keep up. As cybercriminals get smarter, we need smarter defenses. That's where Artificial Intelligence (AI) comes into play. AI is changing the game in web-attack detection, helping us spot and respond to threats in real-time. Let's dive into how cyber-attacks have evolved and how AI is helping to protect us.

Cyber-attacks have come a long way from the simple viruses of the past. Nowadays, they're complex operations that can disrupt essential services and steal sensitive data. Here's a look at some of the most significant modern threats. APTs are like stealthy burglars who break into a network and stay hidden for a long time. Take the "Operation Aurora" attack in 2010, for example. Hackers targeted big companies like Google and Adobe to steal intellectual property and confidential info [1]. These attacks usually go after high-value targets like government agencies and multinational corporations, aiming to swipe sensitive

data or mess up operations. Ransomware attacks involve hackers encrypting a victim's data and demanding payment for the key. With ransomware-as-a-service platforms, it's become easier for criminals to get involved. Remember the 2021 Colonial Pipeline attack? It caused fuel shortages across the U.S. East Coast and showed just how disruptive ransomware can be [2]. These attacks can cripple essential services, leading to widespread chaos.

In supply chain attacks, hackers exploit weaknesses in third-party services or software to break into a target's network. The 2020 SolarWinds incident is a prime example. Attackers injected malicious code into a software update, affecting numerous organizations, including U.S. government agencies [3]. By targeting trusted suppliers, hackers can bypass even robust security measures. Phishing attacks trick people into revealing sensitive info by pretending to be trustworthy entities. According to Verizon's 2020 Data Breach Investigations Report, phishing was involved in 22% of data breaches [4]. Spear-phishing, which targets specific individuals, is even more dangerous because it's personalized. These attacks play on human psychology, making them hard to prevent with technology alone. Zero-day exploits take advantage of unknown software flaws before developers can fix them. The Stuxnet worm, discovered in 2010, used multiple zero-day vulnerabilities to damage Iran's nuclear program [5]. These exploits are highly prized in the cybercriminal world because they can breach even the most secure systems.

Detecting these modern attacks isn't easy:

– *Overwhelming Data*: There's so much network traffic and so many logs that it's nearly impossible to analyze everything manually. A 2020 Ponemon Institute study found that many organizations struggle with the volume of security alerts [6].

– *Sophisticated Tactics*: Hackers use advanced methods like encryption and obfuscation to dodge traditional security tools. Symantec's 2021 report highlights how these tactics help threats slip past defenses [7].

– *Rapidly Evolving Threats*: New cyber threats pop up faster than new security updates can be developed. Gartner noted in 2021 that traditional solutions can't keep up with the pace of emerging threats [8].

– *Human Error*: People can unintentionally compromise security by falling for phishing scams or making mistakes. Human error remains a big factor in breaches, according to Verizon [4].

AI and machine learning are revolutionizing how we detect and respond to cyber threats. Here's how: AI systems learn what's "normal" for a network and can spot when something's off. They analyze user behavior, network traffic, and system operations in real-time. For instance, if there's an unusual login at 3 a.m. from a foreign IP address, AI can flag it. A study in the *Journal of Network and Computer Applications* showed how effective AI is at detecting these anomalies [9].

By looking at historical data, AI can predict potential threats and vulnerabilities. This proactive approach lets organizations fix security gaps before hackers can exploit them. Research by Sari et al. in 2019 emphasized the

importance of predictive analytics in anticipating attacks [10]. AI-powered security tools can automatically respond to threats–like isolating affected systems or blocking suspicious IPs–without waiting for human intervention. IBM Security reported that using AI and automation leads to lower data breach costs and faster response times [11].

AI uses NLP to understand unstructured data, like emails and social media posts, to detect phishing and social engineering attempts. It can catch subtle cues in language that traditional filters might miss. Mawson and Swan (2020) discussed how NLP enhances phishing detection by grasping context and meaning [12]. AI systems get smarter over time by learning from new data. This continuous improvement helps them adapt to emerging threats. Fei et al. (2021) highlighted the benefits of continuous learning in intrusion detection [13].

Benefits of AI in Cybersecurity:

– *Scalability:* AI can handle massive amounts of data, making it ideal for large organizations [14].

– *Speed*: Real-time analysis and quick responses reduce the time systems are vulnerable [15].

– *Accuracy*: Advanced algorithms lower false alarms, so security teams can focus on real threats [16].

– *Efficiency*: Automating routine tasks frees up cybersecurity professionals to tackle more complex issues [17].

Real-World Examples. Darktrace uses AI to detect and respond to cyber threats autonomously. Its Enterprise Immune System learns what's normal for a network and spots anomalies [18]. By acting like a human immune system, it can respond to threats without needing human input.

Google's reCAPTCHA uses machine learning to tell humans and bots apart. This helps protect websites from automated attacks while keeping things user-friendly for real people [19].

IBM's Watson uses AI to analyze security data from various sources, helping analysts respond to threats more efficiently [20]. Its NLP capabilities allow it to understand unstructured data like threat reports and blogs.

Despite its benefits, AI isn't a silver bullet:

– *Adversarial Attacks*: Hackers can use AI techniques to trick or confuse AI systems. Goodfellow et al. (2018) discussed how adversarial inputs can manipulate machine learning models [21].

– *Privacy Issues*: AI needs lots of data, which raises privacy concerns. The European Commission emphasizes balancing innovation with privacy rights [22].

– *Over-Reliance Risk*: Relying too much on AI could make organizations complacent. Human oversight is still crucial. ENISA highlighted the risks of over-dependence [23].

– *Ethical Concerns*: Using AI for surveillance and data analysis must respect individual rights. The IEEE advocates for ethical AI design [24].

Looking ahead:

– *Explainable AI*: Developing AI that can explain its decisions will build trust and help with compliance. Gunning and Aha (2019) stressed the importance of this transparency [25].

– *Tech Integration*: Combining AI with technologies like blockchain could make security even stronger. Gao et al. (2020) discussed how this integration enhances trust [26].

– *Global Collaboration*: Sharing AI-driven threat intelligence can help organizations and governments combat cyber threats together. The World Economic Forum (https://www.weforum.org) suggests that global cooperation is the key.

Conclusions. Cyber-attacks are getting smarter and more complex, which means our defenses need to step up too. AI is playing a crucial role in detecting and responding to these threats, offering capabilities that traditional methods can't match. But while AI brings powerful tools to the table, we need to use it thoughtfully, keeping in mind the challenges and ethical considerations. As cyber threats continue to evolve, embracing AI and doing so responsibly will be essential in staying ahead of the game.

Information sources

1. McAfee. Operation Aurora Hit Google, Others. URL: https://www. mcafee. com, 2010.

2. Cybersecurity and Infrastructure Security Agency (CISA). Colonial Pipeline Cyber Incident. URL: https://www.cisa.gov, 2021.

3. Cybersecurity and Infrastructure Security Agency (CISA). Advanced Persistent Threat Compromise. URL: https://www.cisa.gov, 2020.

4. Verizon. Data Breach Investigations Report. URL: https:// www.verizon. com, 2020.

5. Kaspersky Lab. Stuxnet Analysis Report. URL: https:// www.kaspersky. com, 2010.

6. Ponemon Institute. Cost and Consequences of Gaps in Vulnerability Response. URL: https://www.ponemon.org, 2020.

7. Symantec. Internet Security Threat Report. URL: https:// www.symantec. com, 2021.

8. Gartner. Top Security and Risk Management Trends. URL: https:/ /www. gartner.com, 2021.

9. Chen Y., Li K., & Jiang Y. Survey of Anomaly Detection in Network Security. Journal of Network and Computer Applications, 110, 2018, pp. 128–148.

10. Sari D., Nugroho A. S., & Hidayanto A. N. Predictive Analytics in Cybersecurity. Procedia Computer Science, 161, 2019, pp. 386–392.

11. IBM Security. 2021 Cost of a Data Breach Report. URL: https://www.ibm. com, 2021.

12. Mawson A., & Swan J. Using NLP to Detect Phishing Emails. International Journal of Cybersecurity, 5(2), 2020, pp. 45–53.

13. Fei T., Zhang H., & Wang S. Continuous Learning in Intrusion Detection Systems. Cybersecurity, 4(1), 2021.

14. Accenture. The Future Cybersecurity Workforce Will Be Augmented with AI. URL: https://www.accenture.com, 2020.

15. Cisco. Artificial Intelligence in Cybersecurity. URL: https:// www.cisco.com, 2021.
16. Microsoft. AI in Cybersecurity: A Balancing Act. URL: https:// www.microsoft.com, 2021.
17. Deloitte. AI and the Future of Cybersecurity. URL: https://www2.deloitte. com, 2020.
18. Darktrace. The Enterprise Immune System. URL: https://www.darktrace. com, 2021.
19. Google. reCAPTCHA. URL: https://www.google.com/recaptcha, 2021.
20. IBM. Watson for Cyber Security. URL: https://www.ibm.com, 2021.
21. Goodfellow I., McDaniel P., & Papernot N. Making Machine Learning Robust Against Adversarial Inputs. Communications of the ACM, 61(7), 2018, pp. 56–66.
22. European Commission. White Paper on Artificial Intelligence. URL: https://ec.europa.eu, 2020.
23. European Union Agency for Cybersecurity (ENISA). Artificial Intelligence Cybersecurity Challenges. URL: https://www.enisa.europa.eu, 2021.
24. IEEE. Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. URL: https://ethicsinaction.ieee.org, 2020.
25. Gunning D., & Aha D. DARPA's Explainable Artificial Intelligence Program. AI Magazine, 40(2), 2019, pp. 44–58.
26. Gao J., Shen J., & Liu X. Blockchain and AI Integration for Trustworthy Cybersecurity. IEEE Network, 34(6), 2020, pp. 54–61.

УДК 004.42:004.7(045)

ЗАГРОЗИ CLOUD COMPUTING: ВИКЛИКИ ТА МЕТОДИ ЗАХИСТУ

Христина ОРОЩУК [1]
Наталія МАСЛОВА [1, 2]
Олена ЛЮБИМЕНКО [2]

[1]***Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.***
[2]***Кафедра прикладної математики та інформатики Донецького національного технічного університету, м. Дрогобич, Україна.***

Abstract. *The security issues of Cloud Computing related to the growing popularity of cloud services are discussed, and the main challenges and modern protection methods are explored. A list of the primary types of threats recorded over a decade is presented, highlighting the five most active ones. The basic requirements for cloud service protection are formulated, and the main security tools are outlined. The article emphasizes the need for continuous improvement of security measures in the context of the development of cloud technologies.*

Keywords: *Cloud Computing, security, protection, specialized tools.*

Анотація. *Розглянуті питання безпеки Cloud Computing, пов'язані з ростом популярності хмарних сервісів, досліджено основні виклики та сучасні методи захисту. Сформовано перелік основних типів загроз, зафіксованих за десятирічний період, виділено п'ять найбільш активних. Сформульовано основні вимоги до захисту хмарних сервісів Висвітлено основні інструменти безпеки. Стаття підкреслює необхідність постійного вдосконалення заходів безпеки в умовах розвитку хмарних технологій.*

Ключові слова: *Cloud Computing, безпека, захист, спеціалізовані засоби.*

Хмарні обчислення (Cloud Computing) є невід'ємною частиною сучасних інформаційних технологій, забезпечуючи зручний та постійний доступ до обчислювальних ресурсів, даних і програм. За даними *Statista ma* Eurostat [1, 2], у 2023 році 90% підприємств використовували мультихмарні стратегії для оптимізації роботи та безпеки даних, а 45% підприємств у ЄС впровадили хмарні технології, більшість із яких використовували складні сервіси, такі як хостинг баз даних чи розробка платформ. Згідно прогнозу IDC [3], до 2025 року прогнозується зберігання близько 200 зеттабайтів даних у хмарних середовищах, що вказує на швидкий розвиток цієї галузі.

Однак разом із зростанням популярності хмарних сервісів виникають і проблеми, пов'язані з забезпеченням безпеки Cloud Computing. Захист хмарних обчислень є надзвичайно актуальним питанням, адже від надійності технологій залежить безпека, конфіденційність та цілісність даних великої кількості підприємств й користувачів, стійкість бізнес–процесів та захист критично важливих інфраструктур. У цьому контексті важливо дослідити основні виклики та сучасні методи захисту хмарних структур.

Метою дослідження є визначення ключових загроз та вразливостей хмарних сервісів, класифікація сучасних методів і технологій захисту Cloud Computing.

Основна частина. Першим кроком до організації безпеки хмари є дослідження можливих загроз. Тож розглянемо причини поширення загроз в хмарних обчисленнях.

Першою причиною, слід назвати не належні заходи безпеки з боку користувачів. Як, *наприклад*, слабкі паролі або відсутність шифрування даних, що робить системи вразливими до атак й призводить до зниження рівня безпеки відповідного ресурсу.

По–друге, технологія побудови хмар передбачає спільний доступ до апаратних та програмних ресурсів, що створює ризик витоку даних при обміні між різними користувачами або клієнтами, особливо якщо віртуальні машини недостатньо ізольовані.

Третім фактором назвемо вразливості програмного забезпечення, що включає й використання стороннього програмного забезпечення, й такі загрози, як SQL ін'єкція, Cross–Site Scripting (XSS), IDOR (вразливість, що дозволяє зловмиснику отримати доступ до об'єктів, *наприклад*, файлів чи записів) та інші, які пов'язані з програмами.

Крім того, **х**мари розміщуються в централізованих дата–центрах, які можуть стати метою організованих атак, на кшталт DDoS–атак. Й недоліки належного моніторингу та контролю за доступом до хмарних ресурсів можуть призвести до того, що зловмисники отримають доступ до конфіденційних даних або систем.

Ці фактори ускладнюють забезпечення безпеки хмарних обчислень і створюють ризики для користувачів і організацій.

В процесі дослідження були проаналізовані загрози Cloud Computing, зафіксовані за період з 2010 по 2024 рік й побудована діаграма, яка демонструє активність загроз та підкреслює відносну частоту кожної з них (рис. 1).

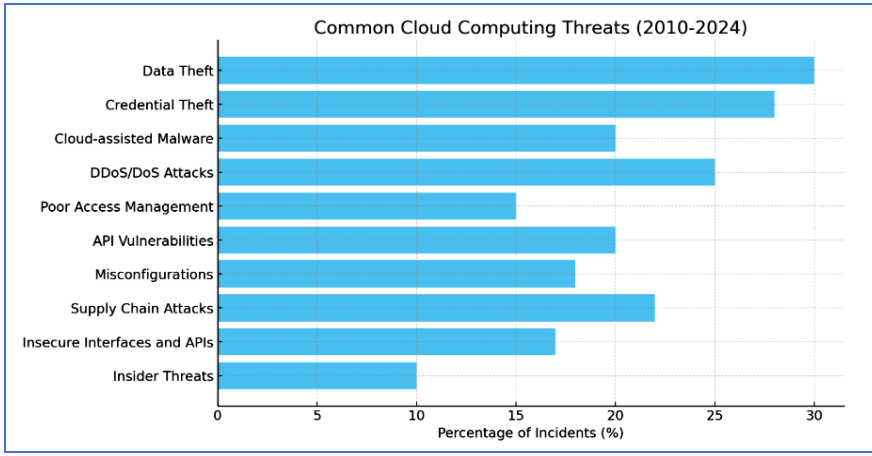


Рис. 1. Загрози Cloud Computing за період 2010–2024р.р.

Так, найбільш характерною загрозою Clod Computing виявилась Data Theft – крадіжка даних. На цю загрозу припадає до 30% інцидентів. Загроза зберігається актуальною з 2010 року і активно зростає разом із розвитком гібридних хмарних інфраструктур [4, 5].

Крадіжка облікових даних (Credential Theft) також одна з найбільш поширених атак, і вона займає важливе місце в хмарних ризиках з 2010 року.

На третьому місці дослідники CSO Online [4] фіксують атаки типу DoS/DDoS. Цей тип атак активно використовуються для ураження хмарних сервісів з 2012 року.

Supply Chain Attacks (Атаки на ланцюги поставок) – це кіберзлочинні атаки, спрямовані на компрометацію продукції або послуг через їхній ланцюг поставок [5]. Відомим прикладом є атака на SolarWinds (2020 рік), коли хакери вставили шкідливий код у програмне забезпечення для управління IT–інфраструктурою, яке використовувалося багатьма урядовими і приватними компаніями.

З 2014 року зловмисники намагаються активно використовувати хмарні сервіси для поширення шкідливого програмного забезпечення, так званого Cloud–assisted Malware, яке також описано в [4]. Й на тому ж п'ятому місті фіксуються вразливості в API та небезпечні інтерфейси, описані в [6].

Тож, і ці загрози, й інші, наведені на рисунку 1 залишаються актуальними протягом десятиріччя, і їх кількість зростає разом із розвитком та складністю хмарних технологій.

Основними вимогами, сформульованими на основі аналізу літературних та статистичних джерел до захисту хмарних сервісів є наступні:

– тотальний захист даних, що зберігаються в хмарі;
– суворі механізми аутентифікації для доступу;
– логічний розподіл й захист каналів віддаленого доступу;
– антивірусний і антиспамовий контроль і перевірка;
– адміністрування та моніторинг ключових систем в режимі 24 × 7;
– всебічний моніторинг і реєстрація;
– балансування навантаження на ключових хмарних системах;
– фізичний захист, відмовостійкість та резервування.

В даному огляді зроблено загальний огляд загроз, без прив'язки до архітектури хмар (IaaS, PaaS, SaaS) та/або моделей розгортання (Private, Public, Hybrid або Community Cloud) тієї чи іншої хмари. Й сама деталізація за конкретною структурою не проводилась, бо метою був саме загальний аналіз й зміна ситуації на протязі десятирічного періода.

Інструментарій захисту. Для захисту файлів, що зберігаються в хмарних сховищах застосовують спеціально створений або адаптований для застосування в Cloud Computing інструментарій. Наведемо основні підходи та інструменти шифрування та безпеки для Cloud Computing [7–9]:

– EncFS (Encfs4Win для Windows) – криптографічна файлова система, яка шифрує файли перед завантаженням у хмару, забезпечуючи конфіденційність;

– пропрієтарне програмне забезпечення на кшталт Boxcryptor, Cloudfogger, TrueCrypt – ці інструменти призначені для шифрування даних у хмарі, що гарантує їх безпеку навіть у разі компрометації провайдера хмарного сховища;

– локальне шифрування за допомогою таких утиліт, як CryptSync, дозволяє зашифрувати файли на локальному пристрої перед синхронізацією з хмарним сховищем;

– програми для резервного копіювання, як Duplicati, пропонують зашифровані рішення для резервного копіювання, забезпечуючи захист даних під час передачі в хмару;

– CarotDav – інструмент, що забезпечує безпечний доступ до хмари та керування файлами, часто використовується для інтеграції з хмарними сервісами, зберігаючи конфіденційність.

Висновки. Хмарні обчислення є невід'ємною частиною сучасних IT-технологій, що забезпечують зручний доступ до обчислювальних ресурсів та даних. Проте з їх поширенням з'являються нові проблеми безпеки, які вимагають постійної уваги та розв'язання. Найбільш поширеними загрозами для хмарних сервісів є крадіжка даних, атаки DoS/DDoS, а також уразливості програмного забезпечення та API. Зокрема, не належні заходи безпеки з боку користувачів та загрози, пов'язані зі спільним доступом до апаратних і програмних ресурсів, створюють додаткові ризики.

Захист хмарних технологій вимагає застосування комплексних заходів, серед яких шифрування даних, надійна аутентифікація, постійний моніторинг та контроль доступу, а також балансування навантаження та фізичний захист серверів. Для забезпечення безпеки даних у хмарах широко використовуються інструменти шифрування, такі як EncFS, Boxcryptor, Cloudfogger, а також програми для резервного копіювання.

Загалом, для ефективного забезпечення безпеки Cloud Computing, необхідно враховувати наявні загрози, постійно оновлювати захисні механізми та впроваджувати новітні та спеціалізовані технології захисту і контролю доступу.

Інформаційні джерела

1. HostingAdvice. (n.d.). Cloud adoption statistics: Trends, forecasts, and strategies. Retrieved November 18, 2024. URL: https://www.hostingadvice.com/how–to/cloud–adoption–statistics/

2. European Commission, Cloud Computing – Statistics on the Use by Enterprises. "Eurostat Statistics Explained, 18 Nov. 2024. URL: https://ec.europa.eu/eurostat/statistics–explained/index.php?title=Cloud_computing_–_statistics_on_the_use_by_enterprises

3. Techjury. (n.d.). How many companies use cloud computing? Retrieved November 18, 2024. URL: https://techjury.net/blog/how–many–companies–use–cloud–computing/

4. Lemos R. (2023, July 10). Top cloud security threats. CSO Online. Retrieved November 19, 2024. URL: https://www.csoonline.com/article/555213/top–cloud–security–threats.html

5. SentinelOne. (2024). Security risks of cloud computing. SentinelOne. Retrieved November 19, 2024. URL: https://www.sentinelone.com/cybersecurity–101/cloud–security/security–risks–of–cloud–computing/

6. Cloud Security Alliance. (2023, September 21). 2023 global cloud threat report: Cloud attacks are lightning fast. Cloud Security Alliance. Retrieved November 19, 2024. URL: https://cloudsecurityalliance.org/blog/2023/09/21/2023–global–cloud–threat–report–cloud–attacks–are–lightning–fast

7. Cloudwards. (n.d.). How to encrypt your data for cloud storage. Cloudwards. Retrieved November 19, 2024. URL: https://www.cloudwards.net/how-to-encrypt-your-data-for-cloud-storage/

8. Horan M. (2013, August 22). Ways to securely encrypt your files in the cloud. Sharetru. URL: https://www.sharetru.com/blog/ways-securely-encrypt-files-cloud

9. Enterprise Storage Forum. (n.d.). Encrypted cloud storage software. Enterprise Storage Forum. Retrieved November 19, 2024. URL: https://www.enterprisestorageforum.com/cloud/encrypted-cloud-storage-software/

УДК 004.056:004.738.5

ВДОСКОНАЛЕННЯ АРХІТЕКТУРИ ЗАСОБІВ АВТОМАТИЗОВАНОГО ПОШУКУ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ

Андрій ІВАНУСА
Артур ТКАЧЕНКО
Андрій ПЕТРОВИЧ

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *WEB application vulnerabilities can include SQL injections, cross-site scripting (XSS), authentication and session management errors, use of vulnerable components, insecure security configurations, etc. Therefore, the development of automated tools to detect such vulnerabilities is critically important to reduce risks. For this purpose, basic algorithms for automated testing have been developed, including algorithms for detecting SQL injections and XSS, which provide effective scanning and detection of potential threats. These algorithms are capable of conducting deep analysis of input data and server responses to detect signs of attacks.*

Keywords: *WEB application, automated search systems, vulnerability scanning, SQL injection algorithm, XSS algorithm, cybersecurity.*

Анотація. *Вразливості WEB-додатків можуть включати SQL-ін'єкції, міжсайтовий скриптинг (XSS), помилки автентифікації та управління сесіями, використання вразливих компонентів, ненадійні конфігурації безпеки тощо. Тому розробка автоматизованих інструментів для виявлення таких вразливостей є критично важливою для зменшення ризиків. З цією метою розроблені базові алгоритми для автоматизованого тестування, включаючи алгоритми для виявлення SQL-ін'єкцій та XSS, забезпечують ефективне сканування та виявлення потенційних загроз. Ці алгоритми здатні проводити глибокий аналіз вхідних даних та відповіді серверів для виявлення ознак атак.*

Ключові слова: *WEB-додаток, системи автоматизованого пошуку, сканування вразливостей, алгоритм SQL-ін'єкцій, алгоритм XSS, кібербезпека.*

Вразливості WEB-додатків – це слабкі місця в системі безпеки, які зловмисники можуть використати для отримання несанкціонованого доступу до конфіденційних даних або порушення цілісності та доступності додатка. Ці вразливості можуть з'явитися під час проєктування та розроблення застосунку або через неадекватні методи забезпечення безпеки під час розгортання та обслуговування [1, 2].

Для розробки інструментів автоматизованого пошуку вразливостей для WEB-додатків потрібна відповідна системна архітектура і компоненти [3, 4].

Нижче наведено рекомендовану системну архітектуру та компоненти для проєктування системи автоматизованого пошуку вразливостей WEB-додатків:

– зовнішній інтерфейс: компонент зовнішнього інтерфейсу відповідатиме за надання користувачам користувацького інтерфейсу. Він надасть користувачам інтерфейс для введення інформації про WEB-додаток. Інтерфейс зовнішнього інтерфейсу має бути простим для навігації та розуміння, а також повинен мати можливість відображати результати сканування вразливостей у чіткій і лаконічній формі;

– бекенд-сервер відповідатиме за зберігання відсканованих даних WEB-додатків, запуск сканерів вразливостей і створення звітів. Бекенд-сервер також повинен мати можливість керувати робочим навантаженням процесу сканування вразливостей;

– сканери вразливостей скануватимуть WEB-додаток на наявність вразливостей. Сканери можуть бути як сторонніми, так і виготовленими за індивідуальним замовленням. Рекомендується використовувати кілька сканерів для підвищення точності результатів сканування;

– база даних буде потрібна для зберігання даних WEB-додатку, результатів сканування вразливостей та іншої відповідної інформації;

– звітність, компонент звітності відповідатиме за створення звітів про сканування вразливостей. Звіти мають бути чіткими та зрозумілими для користувачів;

– безпека має бути ключовим фактором під час розроблення архітектури системи для інструментів автоматичного пошуку вразливостей. Система має бути розроблена з урахуванням вимог безпеки, щоб запобігти несанкціонованому доступу до даних WEB-додатків і результатів сканування вразливостей;

– інтеграція, архітектура системи має бути розроблена для інтеграції з іншими інструментами та системами безпеки, такими як SIEM, щоб забезпечити комплексне рішення для забезпечення безпеки.

Загалом, системна архітектура і компоненти мають бути розроблені таким чином, щоб забезпечити надійний і всебічний автоматизований засіб пошуку вразливостей для WEB-додатків.

Для перехоплення мережевого трафіку зазвичай використовують мережеві карти, переведені в режим прослуховування. Прослуховування мережі Інтернет потребує підключення комп'ютера із запущеним перехоплювачем до сегмента мережі, після чого хакеру стає доступним увесь мережевий трафік, який надсилають і отримують комп'ютери в цьому мережевому сегменті. Ще простіше виконати перехоплення трафіку радіомереж, що використовують бездротові мережеві посередники, у цьому разі не потрібно навіть шукати місце для підключення до кабелю. Або ж зловмисник може

під'єднатися до телефонної лінії, що зв'язує комп'ютер із сервером Інтернету, знайшовши для цього зручне місце. При проходженні авторизації на сайті без шифрування особистих даних, зловмисник при успішному підключенні до мережі підприємства перехоплює особисті дані користувача.

Мережева модель OSI (systems interconnection basic reference model) – це модель взаємодії мережевих протоколів. А протоколи, своєю чергою, це стандарти, які визначають, яким чином обмінюватимуться даними різні програми. Також необхідно передбачити функціональну можливість проєктованої системи виводити звіт її роботи у формі наведеній у таблиці 1.

Таблиця 1.

Звіт за результатами роботи програми

IP адреса	Дата виявлення	Тип вразливості	Підсумок
00.000.00.00	14.10. 2024	Передача даних під час авторизації у відкритому вигляді	Сайт небезпечний, потенційна загроза викрадення даних
…	…	…	…

Висновки. Використання як безпечних, так і небезпечних версій призначеного для користувача WEB-додатка може виявити помилкові спрацьовування та хибні негативні результати сканерів вразливостей. Це може бути пов'язано із методами, які вони використовують. Кореляція між використовуваними методами та виникненням хибних позитивних або хибних негативних результатів може допомогти у визначенні способів покращення методів сканування WEB-додатків.

Інформаційні джерела

1. Open Web Application Security Project [Електронний ресурс]. Дата доступу: 10.11.2024. URL: https://owasp.org/

2. Satapathy S. C., Govardhan A., Raju K. S., Mandal J. K. Виявлення та виправлення ін'єкцій SQL за допомогою методів машинного навчання // Advanced Intelligent Systems Computing. 2015. Вип. 337. – С. 435–442. doi: 10.1007/978-3-319-11191-9_41.

3. Рагвендра Пратап Сінгх, Чандаваркар Б. Р. Генерація динамічної політики безпеки вмісту на стороні клієнта для пом'якшення атак XSS // Матеріали 15-ї Міжнародної конференції з комп'ютерних комунікаційних та мережевих технологій (ICCCNT). 2024. – С. 1–7.

4. Мартінс Н., Круз Дж. М., Круз Т., Абреу П. Х. Змагальне машинне навчання, застосоване до сценаріїв вторгнення та зловмисного програмного забезпечення: систематичний огляд // IEEE Access. 2020. Т. 8. – С. 35403–35419. doi: 10.1109/ACCESS.2020.2975204.

УДК 004.838

ЗАХИСТ КРИПТОВАЛЮТНИХ ГАМАНЦІВ

Максим КОНДРАТЮК
Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *In the modern world, cryptocurrencies are becoming increasingly popular, opening up new opportunities for financial transactions and investments. However, this is accompanied by an increase in the risks associated with theft of digital assets and violation of user security. This work analyzes the main methods of protecting cryptocurrency wallets, including two-factor authentication, the use of hardware wallets, creating backup copies and using reliable exchanges. The emphasis is on the importance of a comprehensive approach to asset protection to minimize the risks of fraud and ensure the safety of investments.*
Keywords: *cryptocurrency, wallet protection, cybersecurity, two-factor authentication, hardware wallets, blockchain, investments, digital assets, cryptography, cryptocurrency exchanges.*

Анотація. *У сучасному світі криптовалюти набувають все більшої популярності, відкриваючи нові можливості для фінансових операцій і інвестицій. Однак це супроводжується зростанням ризиків, пов'язаних із крадіжками цифрових активів та порушенням безпеки користувачів. Ця робота аналізує основні методи захисту криптовалютних гаманців, серед яких двофакторна аутентифікація, використання апаратних гаманців, створення резервних копій та використання надійних бірж. Акцент робиться на важливості комплексного підходу до захисту активів для мінімізації ризиків шахрайства та забезпечення збереження інвестицій.*
Ключові слова: *криптовалюта, захист гаманців, кібербезпека, двофакторна аутентифікація, апаратні гаманці, блокчейн, інвестиції, цифрові активи, криптографія, біржі криптовалют.*

Вступ. У сучасному світі криптовалюти стають дедалі популярнішими, забезпечуючи нові можливості для інвестицій і фінансових операцій. Однак із ростом їхньої популярності зростає й рівень загроз, спрямованих на викрадення криптовалютних активів і компрометацію безпеки користувачів. Захист криптовалютних гаманців стає однією з ключових проблем у сфері кібербезпеки. Важливість ефективних методів і технологій для захисту криптовалютних гаманців є пріоритетом для користувачів та розробників, адже навіть один витік або успішна атака можуть призвести до значних фінансових втрат.

Виклад основного матеріалу. Криптовалюта – це вид цифрової валюти, що застосовує передові методи шифрування, що робить її надзвичайно важкою для фальсифікації. На відміну від традиційних валют, криптовалюти функціонують на основі блокчейну – розподіленої цифрової книги, що пра-

цює незалежно від державного контролю та банківської системи. З моменту появи Bitcoin (BTC) у 2009 році, термін "криптовалюта" виник завдяки використанню шифрування для підтвердження транзакцій. Після цього популярність криптовалют значно зросла, включаючи появу таких валют, як Ether (ETH), Binance Coin (BNB), Tether (USDT) та інших, що привернуло увагу до цих нових цифрових активів [1].

Криптовалютні гаманці являють собою програмні додатки для комп'ютерів і мобільних пристроїв, таких як смартфони або планшети. Вони забезпечують доступ до блокчейн-мережі відповідної криптовалюти через Інтернет. Дані про криптовалюту не зберігаються фізично в гаманці; натомість це фрагменти інформації у розподіленій базі даних, а гаманець збирає ці дані за вашою публічною адресою і відображає баланс у своєму інтерфейсі. Використовуючи такі програми, можна легко надсилати та отримувати криптовалюту, вводячи адресу отримувача, суму, підписуючи транзакцію закритим ключем та додаючи комісію за обробку [2].

Захист криптовалютних активів є критично важливим аспектом для мінімізації ризиків шахрайства та захисту інвестицій. Існують ключові методи забезпечення безпеки криптовалютних гаманців.

Одним із провідних підходів є застосування двофакторної аутентифікації (2FA), що додає додатковий рівень захисту, окрім базових облікових даних. Така функція передбачає використання спеціального коду, який генерується на мобільному пристрої за допомогою додатків, таких як Google Authenticator або Authy. Цей код регулярно змінюється, забезпечуючи підвищений рівень безпеки користувача [3].

Використання холодних гаманців є одним із найефективніших методів захисту криптовалютних активів. Такі гаманці, що зазвичай представлені у вигляді апаратних пристроїв або паперових носіїв, є зашифрованими та мають обмежене підключення до мережі Інтернет, що мінімізує ризики зламів та атак з використанням шкідливого програмного забезпечення. Цей підхід допомагає захистити активи від фішингових атак та вторгнень у біржові акаунти [4].

Регулярне створення резервних копій та оновлення програмного забезпечення гаманця є важливими заходами для захисту даних. Зберігання резервних копій у безпечному середовищі та своєчасне оновлення програмного забезпечення для усунення потенційних вразливостей знижує ймовірність втрати активів [3].

Створення надійних паролів має важливе значення. Рекомендується використовувати унікальні та складні паролі, які раніше не застосовувалися, та зберігати їх у безпечних місцях. Для цього доцільно використовувати менеджери паролів, такі як 1Password або Bitwarden, що дозволяють безпечно зберігати паролі [4].

Вибір надійних криптовалютних бірж також відіграє значну роль у захисті активів. Оцінюючи біржі за показниками безпеки, асортиментом пропонованих активів та відгуками користувачів, платформи на кшталт Bybit, WhiteBIT і Bitfinex демонструють високі стандарти безпеки. Ці платформи використовують 2FA, WAF, а також KYC-верифікацію та AML-перевірку для підвищення рівня захисту активів та мінімізації ризиків шахрайства [4].

При виборі гаманця з максимальним рівнем безпеки важливо враховувати кілька ключових факторів. Апаратні гаманці, такі як Ledger і Trezor, зазвичай вважаються найбільш надійними. Вони зберігають приватні ключі в автономному режимі, що значно ускладнює доступ до ваших коштів для зловмисників. Для тих, хто віддає перевагу зручності, мобільні гаманці, як-от Trust Wallet або Coinbase Wallet, забезпечують оптимальний баланс між комфортом і безпекою.

Леджер. Ці апаратні гаманці пропонують безпечне офлайн-зберігання приватних ключів, захищаючи ваші криптоактиви від онлайн-загроз. Вбудований дисплей і фізичні кнопки для підтвердження транзакцій забезпечують просте та зрозуміле користування.

Трезор. Завдяки сенсорному екрану та розширеним функціям безпеки, гаманці Trezor забезпечують високий рівень захисту приватних ключів та зручний користувацький досвід.

Trust Wallet. Цей мобільний гаманець дозволяє користувачам самостійно контролювати свої приватні ключі, гарантуючи повне право власності на активи. Підтримуючи регулярні оновлення та фокусуючись на безпеці, Trust Wallet забезпечує надійне середовище для зберігання та транзакцій з криптовалютами.

Гаманець Coinbase. Пропонує безпечне рішення для зберігання, зберігаючи більшість активів користувачів у автономному холодному сховищі, що робить їх недоступними для хакерів. Coinbase Wallet також надає повний контроль над приватними ключами користувачів, що забезпечує право власності та мінімізує ризик несанкціонованого доступу [5].

Висновки. Захист криптовалютних гаманців є життєво важливим завданням у сучасному цифровому середовищі. Зважаючи на постійний розвиток кіберзагроз, користувачі повинні усвідомлювати важливість використання сучасних методів і технологій захисту, таких як двофакторна аутентифікація, апаратні гаманці. Крім того, необхідно регулярно оновлювати знання про новітні практики безпеки та бути готовими до адаптації в умовах зміни загроз. Тільки комплексний підхід до захисту цифрових активів дозволить забезпечити безпеку криптовалютних коштів і зменшити ризики несанкціонованого доступу. Впровадження цих заходів допоможе користувачам убезпечити себе та свої активи в умовах зростаючої популярності криптовалют.

Інформаційні джерела

1. Enhancing Security in Cryptocurrency Wallets: Best Practices and Emerging Technologies. URL: https://www.solulab.com/cryptocurrency-wallets-security/ (дата звернення 17.11.2024).
2. Cryptocurrency Wallet: What It Is, How It Works, Types, and Security. URL: https://www.investopedia.com/terms/b/bitcoin-wallet.asp (дата звернення 17.11.2024).
3. Як захистити свій криптогаманець: короткий гайд для новачків. URL: https://speka.media/korotkii-gaid-dlya-novackiv-yak-zaxistiti-svii-kriptogamanec-v7yl7q (дата звернення 17.11.2024).
4. Crypto Wallet Security – A Comprehensive Guide. URL: https://101blockchains.com/crypto-wallet-security/ (дата звернення 17.11.2024).
5. Wallet Security – How to Keep Crypto Wallet Safe. URL: https://evacodes.com/blog/how-to-keep-crypto-wallet-safe#link-7 (дата звернення 17.11.2024).

УДК 004.056.55

РОЗРОБКА МОДУЛІВ І ФУНКЦІОНАЛЬНОСТІ ЗАСОБУ АВТОМАТИЗОВАНОГО ПОШУКУ ВРАЗЛИВОСТЕЙ

Андрій ІВАНУСА
Тарас БРИЧ
Мар'ян ТКАЧ

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *WEB application vulnerabilities may include SQL injections, cross-site scripting (XSS), authentication and session management errors, use of vulnerable components, insecure security configurations, etc. Therefore, the development of automated tools to detect such vulnerabilities is critically important to reduce risks. The developed basic algorithms for automated testing, including algorithms for detecting SQL injections and XSS, provide effective scanning and detection of potential threats. These algorithms are capable of conducting deep analysis of input data and server responses to detect signs of attacks.*

Keywords: *WEB application, automated search systems, vulnerability scanning, SQL injection algorithm, XSS algorithm, cybersecurity.*

Анотація. *Вразливості WEB-додатків можуть включати SQL-ін'єкції, міжсайтовий скриптинг (XSS), помилки автентифікації та управління сесіями, використання вразливих компонентів, ненадійні конфігурації безпеки тощо. Тому розробка автоматизованих інструментів для виявлення таких вразливостей є критично важливою для зменшення ризиків. Розроблені базові алгоритми для автоматизованого тестування, включаючи алгоритми для виявлення SQL-ін'єкцій та XSS, забезпечують ефективне сканування та виявлення потенційних загроз. Ці алгоритми здатні проводити глибокий аналіз вхідних даних та відповіді серверів для виявлення ознак атак.*

Ключові слова: *WEB-додаток, системи автоматизованого пошуку, сканування вразливостей, алгоритм SQL-ін'єкцій, алгоритм XSS, кібербезпека.*

Вразливості WEB-додатків становлять значний ризик для безпеки додатків і конфіденційних даних, з якими вони працюють. Розробники та фахівці з безпеки повинні працювати разом, щоб виявити й усунути ці вразливості та забезпечити безпеку застосунку і його користувачів. Впроваджуючи передові методи безпечної розробки та тестування, організації можуть знизити ризик успішних атак і захистити свої активи від шкоди. У таблиці 1 представлено найпоширеніші вразливості WEB-додатків. У цьому рейтингу представлено тільки шкідливі програми, виключено з нього рекламні програми, які діють вельми настирливо і завдають неприємностей користувачеві, але не завдають шкоди комп'ютеру. Для складання таблиці 1 найбільш поширених вразливостей додатків використано останні доступні дані з OWASP (Open Web Application Security Project), яка регулярно оновлює рейтинг топових вразливостей [1]. Зазначені дані можуть відрізнятися залежно від року та географічного регіону, але загалом вигляді відображають тенденції у сфері кібербезпеки.

Згідно даних [1] найпоширенішими вразливостями WEB-додатків є SQL-ін'єкції, міжсайтовий скриптинг (XSS), підробка міжсайтових запитів (CSRF), зламана автентифікація та управління сесіями, небезпечні прямі посилання на об'єкти.

SQL-ін'єкція – це тип атаки, під час якої зловмисник впроваджує шкідливий код SQL у поля введення програми, щоб отримати несанкціонований доступ до бази даних [2]. Ця вразливість дає змогу зловмиснику переглядати, змінювати або видаляти конфіденційні дані з бази даних. Наслідки успішної атаки шляхом впровадження SQL-коду можуть бути серйозними: від фінансових втрат до компрометації конфіденційної інформації. Щоб запобігти впровадженню SQL, розробники повинні використовувати запити, що містять конкретні параметри і перевірку їх введення, з метою переконання того факту, що введені дані користувачем очищаються додатком перед їх обробкою.

Міжсайтовий скриптинг (XSS) – це тип атаки, під час якої зловмисник впроваджує шкідливі скрипти або код на WEB-сторінку, яку переглядають інші користувачі [3]. Ці скрипти можуть використовуватися для крадіжки конфіденційної інформації або виконання несанкціонованих дій від імені користувача. XSS-атаки можна розділити на дві категорії: збережені та відбиті. Збережені XSS-атаки дають змогу зловмиснику впровадити шкідливий код, який постійно зберігається на сервері, а відбиті XSS-атаки впроваджують код, який негайно відбивається назад користувачеві. Щоб запобігти XSS-атакам, розробники повинні дезінфікувати користувацьке введення і кодувати виведення, щоб запобігти впровадженню скриптів. Крім того, використання Content Security Policy і файлів cookie тільки для HTTP може ще більше знизити ризик XSS.

Підробка міжсайтових запитів (CSRF) – це тип атаки, під час якої зловмисник примушує жертву виконати дію у WEB-додатку без її відома або згоди [4]. Атаки CSRF можуть використовуватися для виконання несанкціонованих дій, таких як зміна пароля жертви або здійснення несанкціонованих покупок. Наслідки успішної атаки CSRF можуть варіюватися від незначних незру-

чностей до серйозних фінансових втрат. Щоб запобігти CSRF, розробники повинні впровадити токени CSRF і управління сеансами, щоб гарантувати, що запити можуть виконуватися тільки авторизованими користувачами.

Враховуючи результати інформаційного аналізу найбільш поширених вразливостей WEB-додатків, порівняльного аналізу методів та технологій виявлення вразливостей було розроблено конкретні алгоритми для виявлення певних вразливостей, таких як SQL-ін'єкція та XSS. Алгоритм проведення автоматизованого пошуку ін'єкцій SQL представлений на рисунку 1.

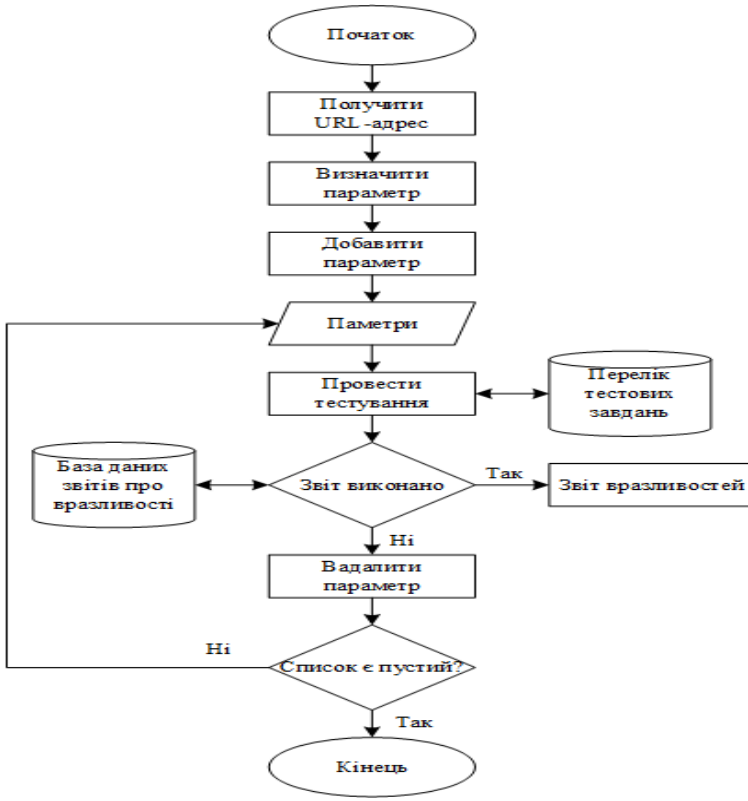


Рис. 1. Алгоритм автоматизованого пошуку SQL-ін'єкцій у проєктованій системі

Для пошуку вразливостей у WEB-додатках, насамперед ініціалізуємо SQL-символи в масиві. Після цього необхідно створити два списки для зберігання повідомлень про помилки SQL:

– один для зберігання повідомлень про помилки конкретної бази даних, таких як повідомлення про помилки SQL тощо;

– інший для зберігання загальних повідомлень про помилки бази даних.

Далі визначаємо значення помилок. Після цього ініціалізуємо метод сканера – сканер приймає повідомлення типу “http”, як введення від шукача. HTTP-повідомлення містить відомості про кожен запит або URL-адресу зі списком параметрів.

Для кожного параметра в повідомленні “http”:

– введемо SQL-символи з масиву;

– перевіримо відповідь, щоб дізнатися чи відповідає вона повідомленням про помилки з двох карт або списків;

– перевіряємо чи відбувається збіг “Flag” та SQL-вразливості;

– у іншому випадку повторюємо дії допоки не буде досягнуто кінця списку параметрів.

Розглянемо розроблений на рисунку 4 алгоритм для XSS. Для кожної URL-адреси в списку відвідуваних URL-адрес:

– визначаємо всі параметри;

– вводимо параметри в список параметрів;

– для кожного параметра в черзі параметрів;

– поставимо сценарій або тестовий приклад XSS як вхідний параметр і передбачаємо передачу запиту;

– перевіримо відповідь, щоб визначити чи наданий сценарій або тестовий випадок;

– повідомляємо про цю вразливість, якщо у відповіді є скрипт.

Висновки. Розробка модулів і функціональних можливостей інструменту призводить до створення комплексного інструменту, який охоплює широкий спектр потенційних вразливостей. Базові алгоритми інструменту забезпечують міцну основу для виявлення вразливостей. Загалом розробка автоматизованого інструменту пошуку вразливостей є важливим кроком на шляху підвищення безпеки Вебдодатків.

Інформаційні джерела

1. Open Web Application Security Project [Electronic resource]. Accessed: 10.11.2024. URL: https://owasp.org/

2. Satapathy S. C., Govardhan A., Raju K. S., Mandal J. K. Detection and remediation of SQL injections using machine learning methods // Advanced Intelligent Systems Computing. 2015. Vol. 337. pp. 435–442. doi: 10.1007/978-3-319-11191-9_41.

3. Raghvendra Pratap Singh, Chandavarkar B. R. Client-side dynamic content security policy generation to mitigate XSS attacks // Proceedings of the 15th International Conference on Computer Communication and Networking Technologies (ICCCNT). 2024. pp. 1–7.

4. Martins N., Cruz J. M., Cruz T., Abreu P. H. Adversarial machine learning applied to intrusion and malware scenarios: a systematic review // IEEE Access. 2020. Vol. 8, pp. 35403–35419. doi: 10.1109/ACCESS.2020.2975204.

УДК 004.056.54

СИСТЕМА ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ТА ЇХ ЗАСТОСУВАННЯ

Богдан ГРАБЧЕНКОВ
Василь ЛУЧИК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The paper examines the two-factor authentication (2FA) system as an effective method of protecting information systems from modern cyber threats. The key principles of 2FA operation, the main types of user verification, and its role in countering phishing attacks, password theft, and social engineering are considered. Promising authentication methods, such as passkeys and biometric data that increase the level of security, are analyzed.*
Keywords: *two-factor authentication, cybersecurity, phishing, social engineering, OTP, hardware tokens, passkeys, biometrics.*

Анотація. *Робота досліджує систему двофакторної аутентифікації (2FA) як ефективний метод захисту інформаційних систем від сучасних кіберзагроз. Розглядаються ключові принципи роботи 2FA, основні види перевірки користувачів, а також її роль у протидії фішинговим атакам, викраденню паролів та соціальній інженерії. Аналізуються перспективні методи аутентифікації, такі як passkeys та біометричні дані, що підвищують рівень безпеки.*
Ключові слова: *двофакторна аутентифікація, кібербезпека, фішинг, соціальна інженерія, OTP, апаратні токени, passkeys, біометрія.*

Сучасний цифровий світ стикається з дедалі більшими загрозами кібербезпеці, які створюють виклики для захисту даних користувачів і корпоративних систем. Парольний захист, як основний засіб аутентифікації, вже не завжди забезпечує належний рівень безпеки через часті випадки витоків паролів та зростаючу складність методів злому. У зв'язку з цим, двофакторна аутентифікація (2FA) стає важливою складовою стратегії забезпечення безпеки. Система двофакторної аутентифікації поєднує два різних рівні перевірки особи, що дозволяє значно підвищити надійність захисту. Поєднання традиційних паролів з додатковими методами, такими як одноразові коди, біометричні дані чи апаратні токени, значно ускладнює доступ зловмисникам.

Двофакторна аутентифікація (2FA) є ключовим компонентом моделі безпеки з нульовою довірою. Для забезпечення захисту конфіденційної інформації необхідно впевнитися, що користувачі, які намагаються отримати доступ до цих даних, справді є тими, за кого себе видають. 2FA є дієвим способом захисту від багатьох загроз безпеці, спрямованих на паролі та об-

лікові записи користувачів, включаючи фішинг, атаки методом грубої сили, крадіжку облікових даних тощо [1].

Двофакторна аутентифікація додає ще один шар захисту до звичайного пароля або PIN-коду для облікових записів, фінансових активів та інших важливих онлайн-акаунтів. При вході в систему користувач має надати два типи підтвердження особи, що значно ускладнює несанкціонований доступ до системи. Актуальність 2FA пояснюється кількома ключовими причинами:

Зростання кіберзагроз. Згідно з дослідженням Rakuten Viber, 81% із 35000 опитаних користувачів стикалися з кібершахраями, а 82% відзначили, що протягом останнього року інтернет-шахрайство стало більш поширеним. Двофакторна аутентифікація створює додатковий бар'єр для зловмисників.

Збереження конфіденційності. 2FA допомагає захистити особисті дані, такі як банківські реквізити, електронні адреси та номери телефонів, які становлять інтерес для шахраїв.

Захист фінансових активів. Двофакторна аутентифікація додає додатковий рівень безпеки для онлайн-банкінгу та електронних платежів [3].

Потреба у двофакторній аутентифікації значно зросла, оскільки компанії, державні установи та широка громадськість розуміють, що одні лише паролі не забезпечують достатнього захисту облікових записів у сучасному технічному середовищі. Середня вартість витоку даних зараз перевищує два трильйони доларів щорічно. Хоча 2FA допомагає захиститися від багатьох загроз, найпоширенішими серед них є:

Викрадені паролі. Звичайний пароль може бути використаний будь-ким, хто отримає до нього доступ. *Наприклад*, якщо користувач записує свій пароль на папері, його можуть викрасти для входу до облікового запису. На відміну від цього, 2FA перевіряє особу користувача через додатковий пристрій після введення пароля.

Соціальна інженерія. Хакери часто маніпулюють людьми, щоб змусити їх розкрити свої паролі. Зокрема, видаючи себе за IT-фахівців, вони можуть завоювати довіру користувача, а потім запитати облікові дані для входу. 2FA захищає від таких атак, здійснюючи перевірку місцезнаходження та IP-адреси після введення пароля.

Фішингові атаки. Хакери часто розсилають електронні листи із посиланнями на шкідливі сайти, які можуть заразити комп'ютер користувача або переконати його ввести свої паролі. Після отримання ці паролі можуть використовуватися для злому. 2FA допомагає боротися з фішингом, додаючи додатковий рівень перевірки після введення пароля [2].

Процес двофакторної аутентифікації зазвичай включає кілька етапів: спочатку користувач вводить своє ім'я користувача та пароль на сторінці

входу. Якщо ці облікові дані правильні, система запитує другий фактор аутентифікації. Користувач повинен надати цей фактор, який може бути:

– Одноразовий пароль: користувач отримує OTP через електронну пошту, SMS або за допомогою мобільного додатка. Цей код потрібно ввести протягом обмеженого часу.

– Апаратний токен: фізичний пристрій, *наприклад*, USB-ключ або NFC-токен, який вставляється або прикладається до пристрою користувача для забезпечення додаткового рівня захисту.

– Push-сповіщення: користувач отримує сповіщення на свій смартфон і підтверджує вхід, натискаючи "підтвердити".

– Passkeys: новий метод автентифікації без паролів, що використовує біометричні дані, такі як відбитки пальців або розпізнавання обличчя. Passkeys зберігають приватні криптографічні ключі на особистому пристрої, забезпечуючи безперервну автентифікацію без необхідності використання OTP або паролів.

Новий метод автентифікації без паролів, що використовує біометричні дані, такі як відбитки пальців або розпізнавання обличчя. Passkeys зберігають приватні криптографічні ключі на особистому пристрої, забезпечуючи безперервну автентифікацію без необхідності використання OTP або паролів. [4].

Висновки. Отже, система двофакторної аутентифікації (2FA) стала одним із найважливіших інструментів у сучасному арсеналі методів кібербезпеки. Вона надійно зміцнює захист інформаційних систем, поєднуючи два незалежні фактори перевірки користувача, що забезпечує значно вищий рівень безпеки порівняно з традиційною аутентифікацією, яка використовує лише паролі. Впровадження 2FA дозволяє ефективно протистояти численним загрозам, зокрема фішинговим атакам, крадіжкам облікових даних та спробам несанкціонованого доступу.

Інформаційні джерела

1. Two-Factor Authentication (2FA). URL: https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa

2. Two Factor Authentication (2FA). URL: https://auth0.com/learn/two-factor-authentication (дата звернення 16.11.2024).

3. Двофакторна автентифікація: як захистити свої дані в епоху кіберзагроз. URL: https://mezha.media/articles/dvofaktorna-avtentyfikatsiia-iak-vstanovyty/ (дата звернення 16.11.2024).

4. Що таке 2FA? Як вибрати найбезпечніший метод двофакторної автентифікації. URL: https://hideez.com/uk-ua/blogs/news/two-factor-authentication-2fa?srsltid=AfmBOoq1uif9nPkpaC8nskbCFNvX7pqVoDQgL3_aqFUPsh50CW6qF_oy (дата звернення 16.11.2024).

УДК 004.056.55:004.738.5

АНАЛІЗ МЕТОДІВ ТА ІНСТРУМЕНТІВ ДЛЯ ПОШУКУ ВРАЗЛИВОСТЕЙ У WEB-ДОДАТКАХ

Андрій ІВАНУСА
Анастасія СОРОКА
Анастасія ЛАНЧЕВИЧ
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *An information analysis of scientific research on the topic of WEB application security was conducted, and it was found that the market lacks high-quality software products for scanning WEB application vulnerabilities. It was found that existing tools do not always effectively detect all types of vulnerabilities, which increases the risk of successful attacks and requires improvement of security approaches. The work includes a system analysis to study vulnerability search methods, a comparative analysis to identify the advantages and disadvantages of manual and automated testing, as well as a system synthesis for developing a software product. Also, a comparative analysis of manual and automated testing showed that although manual testing provides a more detailed analysis and is able to detect complex logical vulnerabilities, automated testing is much faster and better suited for regular scanning of large WEB applications.*

Keywords: *WEB application, automated search systems, vulnerability scanning, SQL injection algorithm, XSS algorithm, cybersecurity.*

Анотація. *Проведено інформаційний аналіз наукових досліджень за темою безпеки WEB-додатків, і встановлено, що на ринку не вистачає якісних програмних продуктів для сканування вразливостей WEB-додатків. Виявлено, що існуючі інструменти не завжди ефективно виявляють усі види вразливостей, що підвищує ризик успішних атак та потребує вдосконалення підходів до забезпечення безпеки. У роботі проведено системний аналіз для вивчення методів пошуку вразливостей, порівняльний аналіз для виявлення переваг і недоліків ручного та автоматизованого тестування, а також системний синтез для розроблення програмного продукту. Також порівняльний аналіз ручного і автоматизованого тестування показав, що хоча ручне тестування забезпечує більш детальний аналіз і здатне виявити складні логічні вразливості, автоматизоване тестування значно швидше і краще підходить для регулярного сканування великих WEB-додатків.*

Ключові слова: *WEB-додаток, системи автоматизованого пошуку, сканування вразливостей, алгоритм SQL-ін'єкцій, алгоритм XSS, кібербезпека.*

Тестування вразливостей – важливий процес забезпечення безпеки WEB-додатків. Він включає в себе виявлення вразливостей у WEB-додатку, які можуть бути використані зловмисниками. Існує два основні методи тестування вразливостей: ручний і автоматичний. Ручне тестування потребує

втручання людини, у той час як автоматизоване тестування використовує програмні засоби для сканування WEB-додатків на наявність вразливостей.

Існують також і різні методи захисту WEB-додатків, деякі з яких є ручними, а інші – автоматизованими. Ручні методи можуть бути ефективними, але вони забирають багато часу і потребують команди фахівців з безпеки. З іншого боку, автоматизовані методи швидші та ефективніші, але вони можуть бути не такими точними, як ручні. Поєднання ручних і автоматичних методів може бути найкращим підходом до забезпечення безпеки WEB-застосунків. Розробка автоматизованого пошуку вразливостей для WEB-додатків може стати перспективним підходом до підвищення ефективності автоматизованих методів.

Однією з суттєвих переваг ручного тестування вразливостей є те, що це ретельний процес, який дає точний результат. Тестувальники можуть використовувати свій досвід, креативність та інтуїцію для виявлення потенційних вразливостей, які можуть пропустити автоматизовані інструменти. Ручне тестування також дає змогу тестувальникам імітувати реальні атаки і розуміти, як зловмисники можуть використовувати вразливості. Крім того, ручне тестування може виявити складні вразливості, які потребують глибокого розуміння архітектури застосунку і сукупності використовуваних технологій.

Автоматичне тестування вразливостей має певні обмеження. Автоматизовані інструменти можуть пропустити деякі вразливості, для виявлення яких потрібне втручання людини. Крім того, автоматизоване тестування не може імітувати реальні атаки, що ускладнює розуміння того, як зловмисники можуть використовувати вразливості. Автоматизоване тестування також обмежене вразливостями, які може виявити інструмент, що ускладнює виявлення складних вразливостей, які потребують глибокого розуміння архітектури застосунку і сукупність взаємозв'язаних технологій. Як ручне, так і автоматизоване тестування вразливостей мають свої переваги та недоліки.

Інструменти автоматизованого тестування вразливостей використовуються для автоматизації процесу виявлення вразливостей і можуть використовуватися для виявлення широкого кола проблем, включно з SQL-ін'єкціями, міжсайтовими сценаріями та іншими вразливостями [1]. Було проведено кілька досліджень з автоматизованого тестування вразливостей для WEB-додатків. Одне з таких досліджень було проведено дослідниками з Каліфорнійського університету в Санта-Барбарі, які розробили інструмент під назвою "Peach Fuzz" для автоматизованого тестування вразливостей. Інструмент був розроблений для виявлення вразливостей у WEB-додатках шляхом створення набору тестових випадків, які можна використовувати для виявлення слабких місць у додатку. Дослідники виявили, що Peach Fuzz зміг виявити кілька вразливостей у WEB-додатках, включно з SQL-ін'єкціями та міжсайтовими сценаріями [2].

Інше дослідження провели дослідники з Університету Меріленда, які розробили інструмент під назвою “WebSSARI” для автоматизованого тестування вразливостей. Інструмент був розроблений для визначення вразливостей у WEB-додатках шляхом аналізу коду та виявлення потенційних вразливостей. Дослідники виявили, що WebSSARI зміг виявити кілька вразливостей у WEB-додатках, включно з SQL-ін’єкціями та міжсайтовими сценаріями [3].

Дослідники з Вашингтонського університету, розробили інструмент під назвою “AppSealer” для автоматизованого тестування вразливостей. Інструмент був розроблений для знаходження вразливостей у мобільних додатках шляхом аналізу коду та виявлення потенційних вразливостей. Дослідники показали, що AppSealer зміг виявити кілька вразливостей у мобільних додатках, зокрема небезпечне зберігання даних, небезпечний зв’язок і небезпечну авторизацію [4].

Ще одне дослідження, провели вчені з Техаського університету в Остіні. Вони розробили інструмент під назвою “Sage” для автоматизованого тестування вразливостей. Інструмент був розроблений для виявлення вразливостей у WEB-додатках шляхом створення набору тестових випадків, які можна використовувати для знаходження слабких місць у додатку. Дослідники показали, що Sage змогла виявити кілька вразливостей у WEB-додатках , включно з SQL-ін’єкцією, міжсайтовим скриптингом та іншими вразливостями [5].

Загалом, автоматизований інструмент пошуку вразливостей повинен надавати комплексне і надійне рішення для виявлення і зниження ризиків безпеки у WEB-додатках.

Вибір оптимального методу розроблення автоматизованого інструменту пошуку вразливостей для WEB-додатків залежить від конкретних потреб і цілей проєкту. Однак комбінація статичного і динамічного аналізу коду часто ефективна при виявленні вразливостей. Крім того, машинне навчання можна використовувати для підвищення точності виявлення вразливостей [6]. Тому доцільно було провести порівняльний аналіз методів виявлення вразливостей WEB-додатків, який представлено у таблиці.

Таблиця 1.

Порівняння методів виявлення вразливостей WEB-додатків

Алгоритм / Метод	Опис	Приклади вразливостей, що виявляються
Сканування сигнатур	Використовує базу відомих сигнатур вразливостей для порівняння з кодом або запитами WEB-додатка. Ефективний для швидкого виявлення відомих вразливостей	SQL-ін’єкції, міжсайтовий скриптинг (XSS), вразливі компоненти
Аналіз поведінки	Аналізує поведінку додатка під час виконання для виявлення нетипових дій або аномалій	Витоки даних, підозрілі операції, зміна прав доступу

Fuzz-тестування	Введення випадкових або помилкових даних у додаток для провокування помилок або некоректної поведінки	SQL-ін'єкції, XSS, буферні переповнення
Статичний аналіз коду (SAST)	Аналіз вихідного коду без виконання додатка для виявлення вразливостей на ранніх етапах розробки	Недостатній контроль доступу, вбудовані паролі, XSS
Динамічний аналіз коду (DAST)	Аналіз додатка під час його виконання. Імітує атаки з метою виявлення вразливостей	SQL-ін'єкції, CSRF, XSS, витік конфіденційних даних
Аналіз потоків даних	Перевіряє, як дані переміщуються між різними компонентами додатка для виявлення небезпечних шляхів	SQL-ін'єкції, витоки конфіденційних даних
Метод "чорної скриньки"	Тестування без доступу до вихідного коду. Виявляє вразливості шляхом імітації атак із зовнішнього середовища	SQL-ін'єкції, XSS, відкриті порти, помилки авторизації
Метод "білої скриньки"	Тестування з повним доступом до вихідного коду та інфраструктури додатка	Логічні помилки, недостатній контроль доступу, бізнес-логіка
Аналіз за допомогою машинного навчання	Використання алгоритмів машинного навчання для виявлення нових і нетипових вразливостей на основі попередніх атак	Аномальні запити, DDoS-атаки, нові форми ін'єкцій
Аналіз на основі шаблонів (Pattern Matching)	Виявлення вразливостей шляхом пошуку шаблонів відомих атак або вразливостей у коді або мережевому трафіку	SQL-ін'єкції, XSS, підробка запитів між сайтами (CSRF)

Інформаційні джерела

1. Dasmohapatra S., Priyadarshini S. B. A comprehensive study on SQL injection attacks, their mode, detection and prevention // Lecture Notes in Networks and Systems. 2021, pp. 617–632. doi: 10.1007/978-981-16-3346-1_50.

2. Son S., McKinley K. S., Shmatikov V. Diglossia: detecting code injection attacks with precision and efficiency // Proceedings of ACM Conference on Computer and Communications Security. 2013. T. 2, pp. 1181–1191. doi: 10.1145/2508859.2516696.

3. Jeffrey S., Foster M., Hicks W., Pugh W. Improving Software Quality with Static Analysis. URL: https://www.cs.umd.edu/~mwh/papers/ paste41gp-foster.pdf.

4. Klein A. Cross Site Scripting Explained. URL: https://pages.cs.wisc.edu/~rist/642-fall-2011/CSS.pdf.

5. Top 10-2025 A05-Security Misconfiguration. Дата доступу: 2024. URL: https://owasp.org/www-project-top-ten/

6. Цигой П., Степанчич Ж., Блажіч Б. Й. Широкомасштабний аналіз WEB-вразливості системи безпеки: висновки, проблеми та способи усунення // Gervasi O., et al. Обчислювальна наука та її застосування – ICCSA 2020. ICCSA 2020. Том 12253. Springer, Cham, 2020. doi: 10.1007/978-3-030-58814-4_64.

Напрям 4

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

UDC 004.056.5: 004.738.5

SECURE DOCUMENT MANAGEMENT VIA VPN IN CORPORATE INFORMATION SYSTEMS

***Ulyana PANOVYK*[1, 2]**
***Roman PANOVYK*[2]**
***Nagaradjan RAJESH*[3]**
***Bohdana FEDYNA*[1, 2]**

[1]Department of Information Security Management, Lviv State University of Life Safety, Lviv, Ukraine.
[2]Department of Computer Technologies in Publishing and Printing Processes, Lviv Polytechnic National University, Lviv, Ukraine.
[3]IS/IT Consultant in IBS, Spain.

Анотація. *Досліджено сучасні технології захисту документообігу в корпоративному середовищі, зокрема можливості VPN для безпечного доступу до документів. Виявлено основні загрози та розглянуто роль VPN у їх мінімізації. Запропоновано VPN-рішення з багатофакторною автентифікацією, контролем доступу та інструментами моніторингу, а також шифруванням і географічними обмеженнями для підвищення надійності з'єднань. Запропоноване VPN-рішення забезпечує вищу надійність та адаптивність порівняно з традиційними методами захисту документообігу.*

Ключові слова: *VPN, безпечний документообіг, корпоративна безпека, багатофакторна автентифікація, контроль доступу, шифрування даних, захист документів.*

Abstract*. Modern technologies for securing document flow in corporate environments have been studied, with a focus on the capabilities of VPNs for secure document access. Key threats have been identified, and the role of VPNs in mitigating these risks has been examined. A VPN solution with multi-factor authentication, access control, monitoring tools, as well as encryption and geographic access restrictions, has been proposed to enhance connection reliability. The proposed VPN solution offers greater reliability and adaptability compared to traditional document security methods.*

Keywords: *VPN, secure document flow, corporate security, multi-factor authentication, access control, data encryption, document protection.*

In today's corporate environment, information is a strategic asset requiring protection at every stage of processing and transmission. With globalization and digitalization, corporate information systems (IS) face security challenges, including unauthorized access, data leaks from network interception, internal

abuses, and external attacks. Traditional network security is insufficient; instead, VPN technology enhances document security through data encryption, user authentication, and access management. As cyber threats grow, VPNs are essential for secure document circulation in corporate IS. This research aims to develop a comprehensive VPN-based approach to help organizations better protect their information resources and minimize confidential data leak risks [1].

Virtual Private Networks (VPNs) are fundamental tools for securing transmitted data within corporate networks. The principle of VPN operation is based on creating an encrypted tunnel through which information is transmitted between remote devices and the organization's central network. This is achieved by encapsulating data packets within a secure tunnel and encrypting them with modern algorithms such as AES (Advanced Encryption Standard). As a result, even if an attacker intercepts the traffic, the data remains inaccessible for decryption. The key elements that ensure reliable VPN operation include user authentication, which restricts access to authorized individuals only; data encryption, which protects information from unauthorized access; and tunneling protocols such as L2TP and PPTP, which provide secure data transmission between the user and the server [2].

The following types of VPNs are commonly used in corporate environments: IPsec VPN (Internet Protocol Security VPN), which provides a high level of security through encryption, authentication, and data integrity, and is often used for inter-office connections over the public Internet infrastructure; SSL VPN (Secure Sockets Layer VPN), which is based on SSL/TLS protocols and provides secure access to corporate resources via a web browser, making it especially convenient for remote users as it does not require specialized client software; and MPLS VPN (Multiprotocol Label Switching VPN), which is used to establish reliable connections between various offices within an organization and ensures fast data routing, making it popular among large corporations with extensive network infrastructures. Specialized systems integrate VPN to ensure secure document circulation. Corporate document management systems, like Microsoft SharePoint, OpenText Documentum, Google Drive, and Microsoft OneDrive for Business, can configure VPN connections for secure access to stored documents. VPN integration provides an extra layer of security, enhancing basic encryption and access management [3].

Document circulation security is a priority in corporate environments, as vulnerabilities in this process can lead to data leaks, loss of confidentiality, and compromised information integrity. Key threats to corporate document circulation include:

– *data interception*: remote connections can become potential points for "man-in-the-middle" (MITM) attacks, where an attacker can intercept and modify data.

– *unauthorized access*: the increasing use of remote and mobile devices complicates access control, heightening the risk of unauthorized access to sensitive information.

– *internal threats*: careless access usage or malicious insider actions can result in data leaks or damage, causing significant harm to the company.

VPN protects data transmission channels, ensuring confidentiality and integrity. Encrypted channels prevent data interception, and decryption without keys is nearly impossible. VPN enhances document security with AES-256 encryption, two-factor authentication, and role-based access control, offering comprehensive protection beyond endpoint encryption [4]. An architectural solution is proposed for secure document circulation through VPN in corporate systems (Fig. 1), providing secure data transmission between remote users and the corporate document server. The primary objective of this architecture is to create an environment that ensures the confidentiality, integrity, and availability of documents within the corporate network.

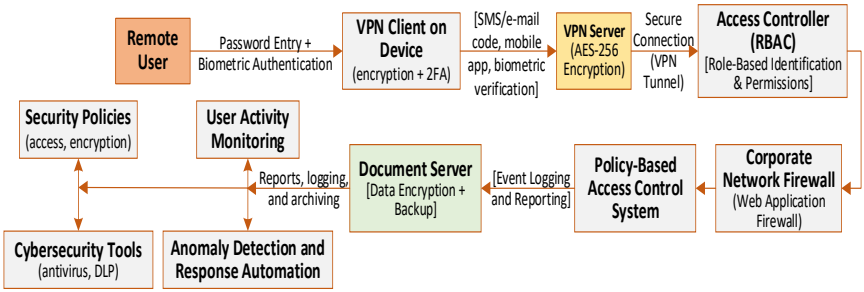


Figure 1 – Diagram of a VPN System for Secure Document Circulation

The key components of the architecture are the VPN server, document server, client devices, and access controller. The VPN server acts as a central node, establishing a secure tunnel between the remote user and the document server, managing user authentication, and encrypting transmitted data. The document server is a secure storage location for corporate documents, accessible only through VPN, adding an extra layer of protection for sensitive data. Client devices are the remote user devices that connect to the corporate network. Each of these devices has a VPN client installed, which automatically creates a secure tunnel when connecting to the corporate server. The access controller administers user access rights based on their roles, defining which documents and resources different user groups can view and edit.

The architecture is based on the principle of “dual verification”, providing an additional layer of security by requiring authentication for each VPN connection. Additionally, all documents transmitted via VPN are encrypted using the AES-256 protocol, which ensures a high level of resistance to hacking. The choice of VPN type for corporate systems depends on the organization’s specifics, usage scenarios, and security requirements; the main options are IPsec and SSL VPN, each offering distinct advantages for different access scenarios.

The secure document access process begins with remote user authentication via multi-factor authentication (MFA), which includes a password and biometric verification for an added layer of security. After authentication, the VPN client on the device establishes an encrypted connection using 2FA and, if possible, biometric checks. The VPN server provides AES-256 encryption for the secure tunnel, allowing data transmission without the risk of interception.

The access controller (RBAC) identifies the user's role and grants access to specific documents, managing rights according to established policies. The corporate network firewall (Web Application Firewall) protects the document server from external threats, such as SQL injections and DDoS attacks. The policy-based access control system further regulates access, blocking it during non-business hours or from suspicious IP addresses. All user actions are logged in an event journal for further reporting and analysis.

Documents on the document server are stored in encrypted form and automatically backed up to prevent data loss. The user activity monitoring system tracks real-time activity, using analytics to detect anomalies. Anomaly detection and response tools automatically restrict access when suspicious activity is detected. Security policies and cybersecurity tools, such as antivirus software and Data Loss Prevention (DLP) systems, protect documents from malware and unauthorized copying. This multi-layered system ensures robust document security through authentication, encryption, access control, and automated response mechanisms.

To ensure document protection, additional security mechanisms and policies are implemented in the system to reduce the risk of unauthorized access. The system includes device control, restricting access only to authorized devices, which reduces the likelihood of using unsecured or personal devices to connect to the corporate network. Another important mechanism is automatic session termination: in case of prolonged inactivity, the system automatically disconnects the VPN, minimizing the risk of unauthorized access. Additionally, geographic access restrictions limit VPN connections to specific regions, protecting against suspicious connections from unusual locations.

The system also employs various security policies, with the primary approach based on role-based access control (RBAC). This approach allocates document access according to employees' functional responsibilities, ensuring that access levels match actual needs. Key security policies include a working hours restriction policy, which allows document access only during business hours, reducing the risk of unauthorized access outside these times. An attempt limit policy is also in place, locking accounts after several failed login attempts, effectively preventing brute-force attacks. Furthermore, IP address and geolocation filtering restricts access to trusted IP addresses and designated regions only. Together, these measures enhance document security, providing a multi-layered defense against both external and internal threats.

Conclusions. These mechanisms ensure that the proposed system provides a high level of document security in a corporate environment, minimizing

unauthorized access risks and safeguarding data confidentiality and integrity throughout all stages of processing and storage. AES-256 encryption and multi-factor authentication securely protect data, significantly reducing the risk of unauthorized access–an aspect often lacking in standard methods. The unified VPN connection optimizes document processing speed, eliminating delays common to traditional approaches. The system's adaptability, including access policies based on working hours and geolocation, enhances its flexibility and alignment with diverse corporate requirements. Thus, the proposed VPN solution offers greater reliability and adaptability compared to traditional document security methods.

Інформаційні джерела

1. Panovyk U. (2024). Cyber security in telecommunication networks and systems. Scientific Papers, № 1(68). pp. 122–135. URL: https://doi.org/10.32403/1998-6912-2024-1-68-122-135/

2. Virtual Private Network (VPN) Security Requirements Guide. STIG Viewer. Unified Compliance Framework. URL: https://www.stigviewer.com/stig/virtual_private_network_vpn_security_requirements_guide/

3. VPN security: How VPNs help secure data and control access. Cloudflare. URL: VPN security: How VPNs help secure data and control access | Cloudflare

4. How to choose and harden your VPN: Best practices from NSA & CISA. Cybersecurity Training & Certifications. Infosec. URL: https://www.infosecinstitute.com/resources/general-security/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/

УДК 004.056.7

РОЛЬ ШИФРУВАННЯ У ЗАБЕЗПЕЧЕННІ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ

Іван САБАДАХ
Василь ЛУЧИК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The role of encryption in ensuring confidentiality and data protection in the digital environment is investigated. The main encryption methods are described, including symmetric and asymmetric algorithms, hash functions and end-to-end encryption. Special attention is paid to the use of encryption in email, databases, cloud technologies and mobile devices to protect against modern cyber threats.*

Keywords: *encryption, confidentiality, symmetric encryption, asymmetric encryption, hash functions, digital signatures, cybersecurity, data integrity.*

Анотація. *Досліджено роль шифрування у забезпеченні конфіденційності та захисту даних у цифровому середовищі. Описуються основні методи шифрування, включаючи симетричні та асиметричні алгоритми, хеш-функції та наскрізне шифрування.*

Особлива увага приділена застосуванню шифрування в електронній пошті, базах даних, хмарних технологіях та мобільних пристроях для захисту від сучасних кіберзагроз.

***Ключові слова**: шифрування, конфіденційність, симетричне шифрування, асиметричне шифрування, хеш-функції, цифрові підписи, кібербезпека, цілісність даних.*

У сучасному цифровому світі, де обмін інформацією відбувається щосекунди, питання конфіденційності та захисту даних набувають особливого значення. Шифрування є одним із найефективніших методів забезпечення безпеки інформації, який допомагає захистити дані від несанкціонованого доступу, крадіжки та підробки. Воно використовується в різних сферах, починаючи від особистого листування і закінчуючи захистом конфіденційної інформації в корпоративних та державних системах. Оскільки сучасні кіберзагрози стають дедалі складнішими, роль шифрування стає надзвичайно важливою у побудові надійних систем безпеки та захисті особистих.

Шифрування – це процес приховування інформації за допомогою спеціального коду. Після шифрування для доступу до даних потрібно знати цей код, щоб здійснити дешифрування. Мета цього процесу – забезпечення доступу до даних лише для тих, хто має відповідний код, роблячи дані недоступними для сторонніх осіб [1].

Шифрування використовується в різних сферах та може включати різні методи, такі як симетричне, асиметричне, хеш-функції та гомоморфне шифрування, кожен з яких адаптований для конкретних потреб безпеки та додатків. Симетричне шифрування передбачає використання одного й того самого ключа для шифрування та дешифрування, що ефективно для великих обсягів даних. Серед прикладів – AES (розширений стандарт шифрування), DES (стандарт шифрування даних) і 3DES (потрійний DES). Асиметричне шифрування базується на парі ключів: відкритому для шифрування та закритому для розшифровки, що дозволяє безпечний обмін без попередньої передачі ключів. Приклади включають RSA (алгоритм Рівеста-Шаміра-Адлемана) і ECC (криптографію еліптичних кривих).

Хеш-функції є односторонніми математичними алгоритмами, що перетворюють вхідні дані у фіксований за розміром байтовий рядок і застосовуються для перевірки цілісності даних та цифрових підписів. Прикладами є SHA-256 і MD5 (остання вважається застарілою та ненадійною для криптографії). Блокові шифри працюють із блоками даних фіксованого розміру, зазвичай 64 або 128 біт, використовуючи симетричний ключ. Приклади – AES і DES. Потокові шифри обробляють дані по біту або байту, що підходить для безперервної передачі даних, *наприклад* RC4 і Salsa20.

Гомоморфне шифрування дозволяє виконувати обчислення над зашифрованими даними без необхідності їх розшифровки, зберігаючи конфіденційність під час обчислень у хмарі. Приклади – шифрування Paillier і повне гомоморфне шифрування (FHE). Наскрізне шифрування забезпечує, що лише сторони спілкування мають доступ до повідомлень і широко використо-

вується в месенджерах та протоколах безпеки, таких як протокол Signal і OTR (Off-the-Record) [2].

Шифрування відіграє ключову роль у забезпеченні безпеки та конфіденційності даних у цифровому середовищі, і його використання охоплює різні сфери, де захист особистої інформації є критично важливим. Основні напрямки застосування шифрування:

Шифрування електронної пошти: захищає електронні листи від несанкціонованого доступу. Протоколи, як-от PGP (Pretty Good Privacy) і S/MIME (Secure/Multipurpose Internet Mail Extensions), забезпечують шифрування та цифровий підпис листів.

Шифрування трафіку: дозволяє захищати передавання даних у мережі. Протоколи HTTPS, SSL і TLS використовуються для шифрування інформації, що передається між веб-сайтами та користувачами, забезпечуючи безпечність онлайн-транзакцій.

Шифрування файлів: допомагає запобігти несанкціонованому доступу до конфіденційних файлів. Інструменти, як-от BitLocker, VeraCrypt і AES, забезпечують шифрування даних на рівні операційної системи чи окремих файлів.

Шифрування баз даних: дозволяє захистити важливі дані в базах даних, використовуючи методи, як-от Transparent Data Encryption (TDE) для SQL Server.

Шифрування зв'язку: месенджери, такі як Signal, WhatsApp і Telegram, застосовують наскрізне шифрування, щоб забезпечити конфіденційність обміну повідомленнями [3].

Шифрування є критично важливим для безпеки даних з таких причин:

1. *Конфіденційність*: дозволяє доступ до даних лише авторизованим користувачам, роблячи їх непридатними для читання без ключа дешифрування. *Наприклад*, під час передавання даних кредитних карток онлайн використовуються протоколи SSL або TLS для захисту від перехоплення.

2. *Цілісність*: шифрування не тільки запобігає несанкціонованому доступу, а й забезпечує збереження даних у незмінному стані. Криптографічні алгоритми дають змогу виявити підроблення даних, *наприклад*, через цифрові підписи для перевірки електронних документів.

3. *Відповідність нормам*: багато галузей мають обов'язкові вимоги щодо захисту даних, де шифрування є необхідним. *Наприклад*, Закон HIPAA вимагає від медичних установ шифрувати дані пацієнтів для захисту конфіденційності.

4. *Безпека в хмарі*: шифрування даних на віддалених серверах захищає їх у разі зламу інфраструктури. Хмарні провайдери, як-от Amazon Web Services (AWS), пропонують служби шифрування, такі як AWS KMS, для захисту даних клієнтів.

5. *Захист мобільних пристроїв*: шифрування забезпечує захист даних на мобільних пристроях у випадку їх втрати чи викрадення. *Наприклад*, пристрої Apple iOS використовують апаратне шифрування, щоб запобігти доступу до даних без пароля [4].

Висновки. Шифрування відіграє критично важливу роль у забезпеченні конфіденційності та захисту інформації у сучасному світі. Використання надійних методів шифрування дозволяє захищати дані від несанкціонованого доступу, забезпечуючи їхню цілісність і захист навіть у випадку перехоплення. Сучасні методи шифрування, такі як симетричні та асиметричні алгоритми, а також постквантові криптосистеми, продовжують вдосконалюватися для того, щоб протистояти новим загрозам. Важливим аспектом залишається грамотне управління криптографічними ключами, що забезпечує додатковий рівень безпеки. Отже, шифрування залишається фундаментальним елементом кібербезпеки та конфіденційності даних. Його правильне застосування та постійне оновлення є запорукою захисту даних у світі, де загрози та технології розвиваються з неймовірною швидкістю.

Інформаційні джерела

1. Protect Data with Encryption. URL: https://www.security.uci.edu/how-to/encryption/ (дата звернення 15.11.2024).
2. How Encryption Safeguards Confidential Information. URL: https://www.drivelock.com/en/blog/encryption (дата звернення 15.11.2024).
3. Роль шифрування у захисті особистої інформації. URL: https://mindscope.biz.ua/rol-shyfruvannya-u-zahysti-osobystoyi-informacziyi/ (дата звернення 15.11.2024).
4. The Role Of Encryption In Safeguarding Your Data. URL: https://fastercapital.com/topics/the-role-of-encryption-in-safeguarding-your-data.html (дата звернення 15.11.2024).

УДК 004.056.2

АНАЛІЗ ЗАГРОЗ У КАНАЛАХ ЗВ'ЯЗКУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ОПЕРАТИВНОЇ ПОЛІГРАФІЇ

Тетяна ГОРДІЄНКО
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *The study examines threats in the communication channels of the network infrastructure for on-demand printing, focusing on risks to customers' confidential data. A hierarchical risk model is proposed to systematize threats, assess their impact, and develop effective protective measures to ensure data security in a digital environment.*

Keywords*: network security, communication channels, e-commerce, operational printing.*

Анотація. *Досліджено загрози у каналах зв'язку мережевої інфраструктури оперативної поліграфії, зокрема ризики для конфіденційних даних замовників. Запропоновано ієрархічну модель ризиків, яка дозволяє систематизувати загрози, оцінити їх вплив і розробити ефективні заходи захисту для гарантування безпеки даних у цифровому середовищі.*

Ключові слова*: мережева безпека, канали зв'язку, електронна комерція, оперативна поліграфія.*

В умовах сучасного ринку, де споживачі очікують максимальної зручності, важливою є коректна інтеграція систем електронної комерції [1] у середовища управління взаємовідносин з клієнтами [2]. В малому і середньому бізнесі оперативної поліграфії [3] такі сервіси дозволяють автоматизувати процес прийняття замовлень, обробки платежів та надання зворотного зв'язку, що суттєво скорочує час на взаємодію з клієнтом і знижує адміністративні витрати. Висока швидкість виконання замовлень є визначальною характеристикою цієї ринкової ніші послуг на вимогу, що вимагає від фірм оптимізації виробничих процесів і взаємодії із замовниками. Важливість впровадження таких рішень обумовлена потребою в забезпеченні безперервності бізнес-процесів, розширенні ринкової аудиторії та підвищенні конкурентоспроможності. Застосування систем електронної комерції дозволяє поліграфічним фірмам не лише адаптуватися до сучасних технологічних змін, а й створювати нові можливості для залучення клієнтів шляхом персоналізації замовлень, автоматизації цінових розрахунків і спрощення логістики.

Оскільки електронна комерція передбачає активну участь клієнтів у процесах створення та передачі замовлень та також здійснення онлайн-оплат, розгортання середовища управління взаємовідносин з клієнтами вимагає забезпечення конфіденційності, цілісності та доступності даних, які замовник надає в процесі взаємодії. Тому, особливу увагу необхідно приділити вибору і застосуванню адекватних засобів захисту інформації в корпоративних каналах зв'язку та комп'ютерних мережах.

Канали зв'язку в корпоративних мережах оперативної поліграфії є одним із ключових елементів інфраструктури, що забезпечує взаємодію між клієнтами, постачальниками послуг і внутрішніми системами. Однак вони також є одними з найуразливіших компонентів, оскільки передача інформації, включаючи конфіденційні дані клієнтів, здійснюється через мережі, що можуть піддаватися різним видам атак. Дослідження загроз у каналах зв'язку мережевої інфраструктури оперативної поліграфії є актуальним з огляду на стрімке зростання залежності цієї галузі від сучасних інформаційних технологій. Використання цифрових інструментів, зокрема систем електронної комерції, для прийняття замовлень, управління процесами та взаємодії з клієнтами потребує високого рівня захисту даних, що циркулюють у корпоративних мережах. Будь-які збої у функціонуванні таких систем можуть призвести до втрати даних, компрометації конфіденційної інформації клієнтів, зниження довіри споживачів та фінансових втрат.

Оперативна поліграфія, орієнтована на швидке виконання замовлень, є надзвичайно чутливою до переривань у роботі інформаційної інфраструктури. Вразливості в каналах зв'язку можуть бути використані для здійснення атак на конфіденційність, цілісність або доступність даних, які є критично важливими для забезпечення якісного надання послуг.

У зв'язку з цим необхідність систематичного дослідження потенційних загроз стає ключовою для підтримки стабільної роботи підприємств

цього сегменту. Укладання ієрархії загроз (рисунок) дозволяє структуровано аналізувати ризики, враховуючи їхній характер, вплив і можливі наслідки для функціонування мережевої інфраструктури. Загрози у каналах зв'язку мережевої інфраструктури оперативної поліграфії вирішено класифікувати за їх впливом на корпоративні дані, а також ризики, пов'язані зі шкідливим програмним забезпеченням. Представлена ієрархія дозволяє комплексно оцінити слабкі місця в інфраструктурі та обґрунтувати заходи для їх мінімізації, ця ієрархія дозволяє систематизувати загрози, з якими стикається мережа оперативної поліграфії, і служить основою для розробки комплексної стратегії захисту.

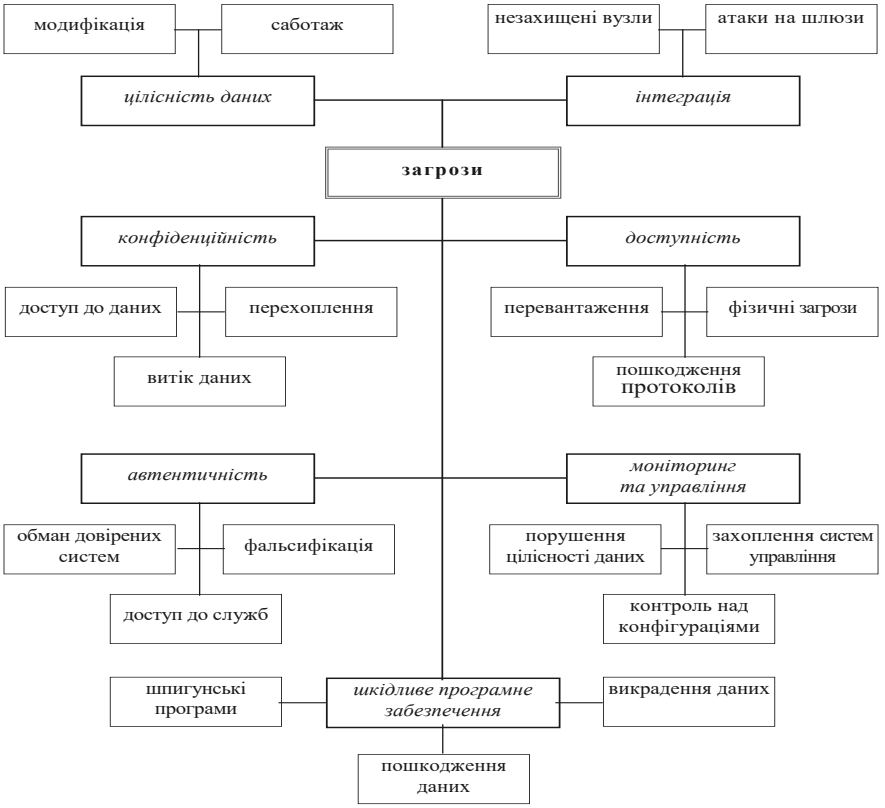


Рисунок 1 – Ієрархічна модель інформаційних ризиків при опрацюванні поліграфічного замовлення

Загрози *конфіденційності* полягають у несанкціонованому доступі до даних, які передаються через канали зв'язку. Основною формою є перехоплення

даних, що здійснюється через пасивне прослуховування трафіку (sniffing) або аналіз метаданих, таких як IP-адреси, обсяги трафіку та часові інтервали.

Це може призводити до витоку інформації про клієнтів чи конфіденційних внутрішніх даних. Інший ризик полягає у використанні незахищених каналів зв'язку, через які зловмисники можуть отримати доступ до даних. Крім того, витоки інформації можливі через незахищені API або зовнішні сервіси, що інтегровані у бізнес-процеси.

Загрози *цілісності спрямовані* на зміну або підробку даних під час їх передачі. Одним із найбільш поширених методів є атака "людина посередині", коли зловмисник перехоплює і змінює інформацію між відправником і отримувачем. Іншим вектором є впровадження підроблених пакетів даних для викривлення комунікації. Саботаж може включати цілеспрямовані зміни конфігурацій мережі або використання шкідливих програм для маніпуляції переданими даними. Загрози *доступності* включають дії, які порушують працездатність мережі чи її компонентів. До них належать атаки на відмову в обслуговуванні (DoS) та розподілені атаки (DDoS), які створюють надмірне навантаження на канали зв'язку. Фізичні пошкодження, такі як обрив кабелів чи перебої в електропостачанні, також знижують доступність мережевих ресурсів. Крім того, можливі атаки на протоколи обміну, які спрямовані на експлуатацію їх уразливостей або маніпуляцію сесіями зв'язку.

Загрози *автентичності* пов'язані з підробкою або компрометацією автентифікаційних механізмів. Це може бути використання підроблених сертифікатів, крадіжка сеансів зв'язку (session hijacking) або брутфорс-атаки на облікові записи користувачів. Фішингові атаки та соціальна інженерія дозволяють обманювати системи автентифікації, змушуючи користувачів розкривати облікові дані або інші чутливі дані. Також можлива експлуатація бекдорів або уразливостей у службах автентифікації. Загрози *інтеграції* виникають через взаємодію з ненадійними зовнішніми вузлами або неправильно налаштованими шлюзами зв'язку. *Наприклад*, підключення через публічні Wi-Fi мережі може створювати ризики перехоплення даних. Шлюзи, такі як брандмауери чи VPN, що мають помилки у конфігурації, можуть стати точкою входу для зловмисників.

Загрози *моніторингу та управління* стосуються маніпуляції або викривлення даних, що використовуються для контролю мережі. Зловмисники можуть впроваджувати шкідливих агентів для підробки даних журналів або атакувати панелі адміністратора для отримання контролю над системами. Відсутність політик регулярного оновлення та тестування конфігурацій створює додаткові ризики. Загрози *шкідливого програмного забезпечення* охоплюють різні типи атак, зокрема шпигунські програми (кейлогери, сніфери), програми для викрадення даних (вимагачі, віруси) та програми для саботажу, такі як хробаки або інші форми шкідливого коду. Ці загрози є універсальними, оскільки можуть бути інтегровані у будь-яку фазу атаки – від початкового вторгнення до завдання шкоди системам чи даним.

Висновки. Виконана систематизація у представленій ієрархії дозволяє глибоко аналізувати потенційні ризики та їхні наслідки для мережевої інфраструктури оперативної поліграфії і є основою для подальшого розгортання ефективної комплексної стратегії захисту із врахуванням багаторівневого характера загроз у каналах зв'язку проєктованого середовища управління взаємовідносин з клієнтами при опрацюванні поліграфічного замовлення із гарантуванням інформаційної безпеки, особливо в умовах цифровізації оперативної поліграфії.

Інформаційні джерела

1. Балик У. О., Колісник М. В. Електронна комерція як елемент системи світового господарства. Вісник НУ "ЛП": Логістика, №811, 2014. – С. 11–19.

2. Богоявленський О. В. Управління процесами взаємовідносин з клієнтами як фактор підвищення конкурентоспроможності вітчизняних підприємств та їх продукції. Зовнішня торгівля: економіка, фінанси, право, №2, 2014. – С. 73–81.

3 Патала О. Мережева інфраструктура інформаційної системи центру оперативної поліграфії. Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті, №6, 2018. – С. 95–97.

УДК 004.838

МЕТОДИ ЗАХИСТУ ІОТ-ПРИСТРОЇВ ВІД КІБЕРЗАГРОЗ

Віталій СВІТЛИЧНИЙ
Віталій ШЕСТАКОВ

Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article reviews the current state of the Internet of Things (IoT) and the related cybersecurity challenges that are becoming increasingly relevant due to the rapid growth of the number of connected devices. The main risks associated with vulnerabilities in IoT systems are analyzed and the possible consequences of cyberattacks are highlighted, including data theft, system compromise, and threats to critical infrastructure. The importance of implementing security strategies such as data encryption, user authentication, software updates, network segmentation, and the use of modern security protocols is emphasized. The described measures can significantly increase the security of IoT networks and minimize potential threats.*

Keywords: *Internet of Things (IoT), cybersecurity, cyberattacks, data protection, encryption, authentication, software updates, network segmentation, device management, cyberthreats.*

Анотація. *У статті розглянуто сучасний стан Інтернету речей (IoT) і супутні виклики кібербезпеки, що стають дедалі актуальнішими через швидке зростання*

кількості підключених пристроїв. Аналізуються основні ризики, пов'язані з уразливостями IoT-систем, і висвітлюються можливі наслідки кібератак, зокрема крадіжка даних, компрометація систем та загрози для критичної інфраструктури. Підкреслюється важливість впровадження стратегій захисту, таких як шифрування даних, автентифікація користувачів, оновлення програмного забезпечення, сегментація мереж і використання сучасних протоколів безпеки. Описані заходи можуть суттєво підвищити безпеку IoT-мереж та мінімізувати потенційні загрози.

Ключові слова: *Інтернет речей (IoT), кібербезпека, кібератаки, захист даних, шифрування, автентифікація, оновлення програмного забезпечення, сегментація мереж, управління пристроями, кіберзагрози.*

У сучасному світі Інтернет речей (IoT) став невід'ємною частиною повсякденного життя, об'єднуючи мільярди пристроїв, які полегшують наш побут, бізнес-процеси та управління інфраструктурою. Однак із збільшенням кількості підключених пристроїв виникає гостра проблема кібербезпеки. IoT-пристрої часто мають обмежені можливості захисту, що робить їх привабливими цілями для кіберзлочинців, здатних використовувати їх для крадіжки даних, компрометації систем та навіть організації великих кібератак.

Враховуючи важливість і широту застосування IoT, питання розробки та впровадження ефективних методів захисту таких пристроїв стає першочерговим завданням для фахівців з кібербезпеки. Основними викликами є забезпечення безпеки передачі даних, захист від несанкціонованого доступу, а також виявлення і нейтралізація загроз у реальному часі.

Інтернет речей (IoT) – це сукупність взаємопов'язаних пристроїв, які взаємодіють один з одним для виконання різних завдань у сфері побуту, промисловості, бізнесу та інших галузях. IoT значно змінив наше повсякденне життя, робочі процеси та спосіб комунікації з оточуючим світом. Однак зі зростанням кількості IoT-пристроїв збільшується і ймовірність кібератак. Хакери можуть скористатися вразливостями цих пристроїв, щоб отримати доступ до конфіденційної інформації або взяти під контроль критичні системи. Додатковою проблемою є централізована структура IoT-мереж, що робить їх вразливими до атак із єдиною точкою відмови [1].

За даними Statista, кількість розумних пристроїв, здатних передавати дані через Інтернет, вже перевищує 18 мільярдів у всьому світі. Дослідження Unit 42 показує, що 98% цих пристроїв передають дані у незашифрованому вигляді, що підвищує їхню вразливість. Як результат, лише в першій половині 2023 року кількість атак на IoT зросла до 77,9 мільйонів, що на 37% більше, ніж у той же період 2022 року. Звіт Keyfactor також підтверджує серйозність загрози: 97% організацій, що використовують IoT-пристрої, зазнавали кібератак, з яких 89% понесли фінансові збитки, а 69% відзначили зростання тиску через постійні злами. Отже, ризик кібератак для кожного є цілком реальним [2].

Зважаючи на вразливість IoT-мереж і серйозні наслідки можливих атак, важливо заздалегідь впроваджувати ефективні заходи для зниження ризиків. Ось шість основних стратегій для захисту IoT-пристроїв від кіберзагроз.

Захист Wi-Fi роутера. Як повідомляє ESET, важливим кроком для забезпечення безпеки інтернет-з'єднання є захист роутера, який виступає ключовим пристроєм в інфраструктурі Інтернету речей. Часто користувачі залишають налаштування роутера за замовчуванням після його встановлення, що є поширеною помилкою та серйозною загрозою для безпеки підключених пристроїв. Тому зміна паролів для підключення до роутера та доступу до його налаштувань має бути першочерговим завданням [3].

Шифрування даних. Шифрування є перевіреним методом захисту інформації, який зберігає свою актуальність і сьогодні. Сучасні технології використовують надійні стандарти, такі як AES, RCA та ECC. Крім того, для захисту передачі даних застосовуються протоколи безпечного зв'язку, як-от TLS (Transport Layer Security). Також враховуються окремі рішення для захисту даних як у стані спокою (at rest), так і під час передачі (in transit). Важливо забезпечити правильне керування криптографічними ключами, які повинні зберігатися у безпечному середовищі. Для підвищення безпеки можуть застосовуватися апаратні модулі безпеки (HSM). Регулярне оновлення ключів та використання унікальних ключів для кожної моделі пристрою допомагає знизити ризик компрометації даних [2].

Автентифікація та контроль доступу. Одним із ключових принципів захисту під час реєстрації IoT-пристроїв є використання складних, унікальних паролів, які повинні бути достатньо довгими та містити великі й малі літери, цифри та спеціальні символи. Уникнення використання однакових паролів для різних пристроїв є важливим аспектом безпеки. Додаткові заходи, як-от двофакторна автентифікація, передбачають введення додаткового коду або підтвердження через мобільний пристрій для доступу до системи. Також рекомендовано регулярно оновлювати програмне забезпечення пристрою, адже виробники постійно випускають оновлення для усунення виявлених вразливостей [4].

Оновлення та патчинг програмного забезпечення. Використання застарілого програмного забезпечення може не лише погіршити функціонування пристрою, а й створити нові вразливості, якими можуть скористатися зловмисники. Тому надзвичайно важливо, щоб виробники підтримували свої пристрої протягом усього їхнього життєвого циклу, регулярно випускаючи оновлення та оперативно виправляючи помилки за допомогою патчів. Вони повинні інформувати користувачів про наявність нових версій та важливість їх ручної установки. Однак найбільш ефективним рішенням є впровадження автоматичного оновлення, яке працює без втручання корис-

тувача. Це має відбуватися з дотриманням вимог безпеки, зокрема перевіркою підпису виробника для запобігання підміні програмного забезпечення. У великих компаніях системні адміністратори можуть використовувати централізовані системи для управління оновленнями на численних пристроях, що забезпечує однорідність IT-інфраструктури та значно знижує кількість вразливостей, одночасно зменшуючи витрати на утримання та обслуговування обладнання [2].

Захист смартфона є важливим аспектом безпеки, оскільки сучасні мобільні пристрої мають безліч функцій і використовуються не тільки для дзвінків, але й для фотографування, зберігання файлів, відправки та отримання електронної пошти, а також виконання інших завдань, пов'язаних із доступом до особистих даних і підключенням до Інтернету. Тому смартфон потребує надійного захисту. Більшість смартфонів обладнані вбудованими засобами безпеки, які допомагають запобігти загрозам. Проте для посилення захисту рекомендується шифрувати всі конфіденційні дані, щоб у разі несанкціонованого доступу зловмисники не змогли отримати доступ до особистої інформації. Більш детальні поради щодо захисту смартфона можна знайти за відповідним посиланням [3].

Сегментація мережі. Сегментація – це метод цифрової ізоляції, який дозволяє розділяти різні типи IoT-пристроїв у межах однієї мережі. Поділ мережі на окремі логічні або фізичні сегменти з власними правилами безпеки та обмеженнями доступу допомагає мінімізувати можливі наслідки атак для всієї інфраструктури. Це особливо важливо для розподілених мереж, що обслуговують великі підприємства та організації. Сегментація також покращує управління IT-інфраструктурою та підвищує продуктивність, зменшуючи обсяг трафіку між різними секціями. Класичним рішенням для контролю трафіку між сегментами є використання віртуальних локальних мереж (VLAN) та налаштування правил брандмауера. Окрім цього, застосовується підхід Zero Trust ("нульова довіра"), за яким жоден пристрій або користувач не отримують автоматичного доступу, а кожна сесія повинна бути перевірена та авторизована [2].

Таблиця 1

Аналіз сервісів та інструментів для захисту IoT пристроїв від кіберзагроз

Сервіс/ Продукт	*Основні функції*	*Сумісність з пристроями*	*Методи захисту*	*Розгортання*	*Виробник*
AWS IoT Core	Безпечне двостороннє спілкування, управління мільйонами пристроїв	Широкий спектр протоколів, різноманітні пристрої IoT	Шифрування даних, автентифікація пристроїв	Хмара	Amazon Web Services

Azure IoT Hub	Безпечне двостороннє спілкування, управління мільйонами пристроїв	Широкий спектр протоколів, різноманітні пристрої IoT	Шифрування даних, автентифікація пристроїв, авторизація доступу	Хмара	Microsoft
Google Cloud IoT Core	Безпечне двостороннє спілкування, управління мільйонами пристроїв	Широкий спектр протоколів, різноманітні пристрої IoT	Шифрування даних, автентифікація пристроїв, авторизація доступу	Хмара	Google Cloud Platform

Висновки. Отже, розвиток IoT-технологій супроводжується зростанням ризиків, пов'язаних із кіберзагрозами. Незахищені IoT-пристрої можуть стати легкою мішенню для хакерів, що призводить до компрометації даних, порушення приватності та загроз безпеці важливих систем. У цьому контексті особливу важливість мають ефективні методи захисту IoT, які включають використання складних паролів, впровадження двофакторної автентифікації, регулярне оновлення програмного забезпечення та моніторинг мережевої активності. Таким чином, для забезпечення надійного захисту IoT-систем необхідно впроваджувати сучасні методи кібербезпеки, враховувати специфіку пристроїв та активно реагувати на нові виклики в сфері кіберзагроз. Лише завдяки скоординованим діям користувачів, розробників та фахівців з кібербезпеки можна мінімізувати ризики та забезпечити безпечне функціонування Інтернету речей у різних сферах діяльності.

Інформаційні джерела

1. Як захистити Інтернет речей за допомогою Blockchain. URL: https://www.hx.technology/ua/blog-ua/how-secure-internet-of-things-with-blockchain-ua (дата звернення 10.11.2024).

2. Кіберзагрози для інтернету речей (IoT): захист смарт-пристроїв. URL: https://wezom.com.ua/ua/blog/kiberzagrozi-dlya-internetu-rechey-iot-zahist-smart-pristroyiv (дата звернення 10.11.2024).

3. Як посилити захист Інтернету речей – базові кроки. URL: https://www.eset.com/ua/about/newsroom/blog/smart-technologies/kak-usilit-zashchitu-internet-veshchey-bazovyye-shagi/?srsltid=AfmBOooSSq46D8IwLfQWlKq7l4HshrjVlMtUaZ7_buAUYZT oQbifwGVo (дата звернення 10.11.2024).

4. Основні принципи та рекомендації щодо захисту реєстрації IoT-пристроїв від кіберзагроз. URL: https://mediacom.com.ua/zaxist-reestratsii-iot-pristroiv-osnovni-printsipi-ta-rekomendatsii/ (дата звернення 10.11.2024).

УДК 32.019.51

АКТУАЛЬНІСТЬ ЗАХИСТУ Й БЕЗПЕКИ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ І МЕСЕНДЖЕРАХ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

Тетяна КЛИМЕНКО
Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут", м. Харків, Україна.

Abstract. *The relevance of information protection and security in social networks and messengers in conditions of martial law is becoming very important in the modern world. Thanks to the development of technology, information can be stolen, distributed without permission and used for provocations and disinformation. In such conditions, additional security measures must be taken.*
Keywords: *threat, protection, information, messenger, digital security, encryption.*

Анотація. *Актуальність захисту й безпеки інформації в соцмережах і месенджерах в умовах військового стану стає вельми важливою у сучасному світі. Завдяки розвитку технологій, інформація може бути вкрадена, поширена без дозволу та використана для провокацій та дезінформації. У таких умовах необхідно вживати додаткові заходи безпеки.*
Ключові слова: *загроза, захист, інформація, месенджер, цифрова безпека, шифрування.*

У сучасному світі складно уявити життя без соціальних платформ. Месенджери настільки глибоко інтегровані в наше повсякденне життя, що стали його левовою частиною. У чатах ми обговорюємо особисті й робочі питання, витрачаючи на переписування доволі багато часу. Наші акаунти містять інформацію, яка потребує надійного захисту.

Захист і безпека інформації у соцмережах та месенджерах стають надзвичайно важливими в умовах військового стану. У таких умовах інформація може бути використана для ворожих дій або шпигунства. Для захисту інформації варто дотримуватись наступних правил:

– використання надійних паролів та двофакторної аутентифікації для власних акаунтів;

– заборона розповсюдження конфіденційної інформації у відкритих чатах або публічних постах, особливо в умовах конфлікту;

– відстежування джерела інформації та перевірка її достовірності перед поширенням;

– використання енкрипції: встановлення захищених месенджерів для конфіденційних розмов та шифрування повідомлень з подальшим їх видаленням;

– уникнення натискання на посилання від невідомих джерел;

– заборона викладання місцезнаходження: уникнення надсилання фото або інформації про точне місце перебування.

Ці прості правила допоможуть зберегти інформацію в безпеці навіть у складних умовах військового стану.

Тож де саме безпечно листуватися, щоб уникнути злому й інших небезпек?

За результатами Глобального оглядового звіту Digital 2023 найпопулярнішими у світі мобільними месенжерами за кількістю щомісячних активних користувачів (млн.) є WhatsApp (2000), Weixin/WeChat (1309), Facebook (931), Telegram (700), Snapchat (635), QQ (574) [1].

Щодо наших співвітчизників, то українці масово оволоділи месенджерами Viber, WhatsApp і Telegram.

Однак треба пам'ятати, що сервери компанії Viber розташовані в росії. Проте в компанії стверджують, що на них знаходяться лише дані російських користувачів. Гарантій, що дані українських користувачів не зберігаються в тому ж місці, немає, бо цю інформацію перевірити неможливо.

WhatsApp для посилення захисту інформації запровадив наскрізне шифрування, для реалізації якого використовується бібліотека месенджера Signal, який прийнято вважати найбільш безпечним у світі. Однак експерти не радять повністю довіряти месенджеру через приналежність компанії Facebook з агресивними механізмами отримання інформації про користувачів. У Telegram є два варіанти шифрування: для звичайних і для секретних чатів. Розробники стверджують, що інформація звичайних чатів зберігається на кількох серверах по всьому світу і контролюється різними законами з надання доступу до неї. Ключі для розшифровки також зберігаються окремими блоками на різних серверах. Однак лише секретні чати підтримують end-to-end-шифрування.

Telegram не є безпечним і зашифрованим застосунком, все частіше з'являються факти злому акаунтів, також існують факти потенційного доступу ФСБ до переписок користувачів.

За статистикою умовно безпечними месенджерами для нас на сьогодні є Signal і WhatsApp. Найбільш захищеним месенджером вважається Signal. В ньому вся інформація зашифрована. Повідомлення зберігаються на пристрої й локально шифруються за допомогою парольної фрази перед відправкою на сервер [1].

Signal має конкурентів, але ж вони не є безкоштовними. Це популярний у Європі месенджер Threema, який приділяє багато уваги безпеці. При першому відвідуванні додатка користувач водить пальцем по екрану, щоб згенерувати свій унікальний ідентифікатор. Всі повідомлення шифруються прямо на пристрої, а прочитати їх може лише одержувач. Інший месенджер – Silent Phone. Він пропонує криптографічний захист передачі голосових, текстових, відеоповідомлень і файлів до 100Мб. Месенджер Confide позиціонує себе як зашифрований і захищений від скріншотів. Він дозволяє обмінюватися повідомленнями, що зникають, а також гарантує спілкування без ризику того, що бесіда буде збережена або кому-небудь переслана. Всі повідомлення після прочитання автоматично втрачаються назавжди [2].

Позитивна відмінність популярних месенджерів у тому, що вони дозволяють зберігати повідомлення, щоб уникнути втрати даних. Негативна – саме відсутність такої функції робить захищені месенджери безпечними.

Отже, коли йдеться про безпечне листування, завжди краще використовувати шифрування end-to-end (кінця до кінця), яке гарантує, що повідомлення залишаються приватними. Популярні месенджери, які надають цю можливість, – це Signal, WhatsApp (якщо ввімкнено шифрування) і Telegram (використовуючи "секретні чати"). Але ж треба пам'ятати, що жоден месенджер не може гарантувати 100% захисту даних. Спецслужби та різні розвідувальні агенції на сьогодні теоретично та практично можуть контролювати практично будь-який централізований месенджер та продублювати будь-яку SIM-картку або перехопити SMS. В сучасних умовах досягти абсолютної анонімності дуже складно і дуже дорого, а іноді неможливо [2].

Висновки. Важливо бути обережними при обміні чутливою інформацією та завжди перевіряти адреси отримувачів, щоб уникнути шахрайства та інших загроз. Користувачі регулярно мають навчатися та дізнаватися про нові загрози та методи забезпечення цифрової безпеки, щоб бути в курсі та захищати себе, адже безпека – це не статичний стан, а безперервний процес, який вимагає регулярних заходів і перевірок.

Інформаційні джерела

1. Telegram, Viber, WhatsApp, Signal – яким месенджерам можна довіряти, 2023. URL: https://www.epravda.com.ua/publications/ 2017 /12/15/632183/.

2. У пошуках безпечного месенджера, 2023. URL: https://kr-labs.com.ua/blog/top-secure-and-privacy-messaging-apps.

УДК 004.93:004.738.5

ОЦІНЮВАННЯ ВРАЗЛИВОСТЕЙ У ВІРТУАЛЬНИХ СЕРЕДОВИЩАХ З ВИКОРИСТАННЯМ ПЛАТФОРМИ TRYHACKME

Валентина ЯЩУК
Назар КУТНИК
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The theoretical, scientific, methodological, organizational and functional bases of using the TryHackMe platform to study virtual machine vulnerabilities are considered. Modern approaches to cybersecurity training based on controlled environments are identified. Methodological approaches to the formation of the concept of vulnerability assessment in virtual environments used on the platform are presented. The stages of solving the scientific and practical problem of vulnerability research are proposed.*

Keywords: *virtual machines, TryHackMe, vulnerabilities, cybersecurity, penetration testing, security configuration.*

Анотація. *Розглянуто теоритичні, науково-методичні та організаційно-функціональні основи використання платформи TryHackMe для вивчення вразливостей віртуальних машин. Визначено сучасні підходи до навчання кібербезпеки на базі контрольованих середовищ. Наведено методичні підходи до формування концепції оцінювання вразливостей у віртуальних середовищах, які використовуються на платформі. Запропоновано етапи вирішення науково-практичної проблеми дослідження вразливостей.*

Ключові слова: *віртуальні машини, TryHackMe, вразливості, кібербезпека, тестування на проникнення, конфігурація безпеки.*

Платформа TryHackMe є одним із провідних інструментів для навчання кібербезпеці. Вона надає користувачам можливість практично відточувати свої навички в безпеці мереж, веб-додатків, операційних систем та інших сферах. Віртуальні машина на платформі TryHackMe використовуються для навчання та розвитку навичок кібербезпеки. Вони спеціально створені з вразливостями, які служать тренувальним полігоном для майбутніх спеціалістів у галузі кібербезпеки. Ці середовища дозволяють практикувати різні методи тестування на проникнення, аналізу безпеки та оцінки вразливостей у безпечному та контрольованому контексті. Завдяки TryHackMe студенти та фахівці можуть не тільки знайомитися з теоретичними аспектами кібербезпеки, але й відпрацьовувати практичні навички, які є критично важливими для сучасної галузі інформаційної безпеки.

Платформа TryHackMe є чудовим прикладом того, як сучасні навчальні інструменти допомагають створювати реалістичні симуляції кіберзагроз та дозволяють студентам відчути себе на місці атакуючого або захисника. Навчальні віртуальні машини, які використовуються на платформі, створюються з різними видами вразливостей, спеціально залишеними для того, щоб користувачі могли знаходити та аналізувати ці слабкі місця. *Наприклад*, неправильні конфігурації систем, застаріле або некоректно налаштоване програмне забезпечення, слабкі механізми аутентифікації та відкриті порти. Ці аспекти є основними цілями для аналізу на платформі, і вони допомагають краще зрозуміти, як зловмисники можуть скористатися цими вразливостями для проникнення у системи.

Для успішного навчання кібербезпеці користувачі TryHackMe мають можливість використовувати різноманітні методи для виявлення та оцінки вразливостей. Одним з основних підходів є сканування мережевих портів і служб за допомогою таких інструментів, як Nmap. Це дає змогу виявляти відкриті порти, які можуть використовуватися для несанкціонованого доступу, а також визначати активні служби, що можуть містити потенційні слабкі місця. Окрім сканування, важливим є також аналіз журналів подій та моніторинг мережевої активності, що дозволяє виявляти підозрілі дії, несанкціоновані доступи та інші аномалії. Тестування проникнення, яке зазвичай проводиться після виявлення вразливостей, дає можливість оцінити, наскільки ефективно налаштовані системи захисту та як легко вони можуть бути обійдені.

Однією з важливих переваг платформи TryHackMe є доступ до різноманітних навчальних сценаріїв, які охоплюють широкий спектр можливих атак. Це включає практику роботи з такими вразливостями, як SQL-ін'єкції, міжсайтовий скриптинг (XSS), експлуатація відомих вразливостей програмного забезпечення, атаки на мережеві протоколи, соціальна інженерія тощо. Такі сценарії дають можливість відпрацьовувати практичні навички в умовах, максимально наближених до реальних. Завдяки цьому майбутні фахівці отримують досвід у виявленні, аналізі та усуненні вразливостей, що є надзвичайно важливим у сучасній кібербезпеці.

Попри навчальний характер віртуальних машин на платформі, важливо розуміти, що принципи захисту залишаються актуальними навіть у таких умовах. Оскільки здобувачі вчаться не тільки шукати вразливості, а й захищати системи, необхідно враховувати рекомендації щодо забезпечення належного рівня безпеки. Це включає регулярне оновлення програмного забезпечення, своєчасне встановлення патчів безпеки, впровадження суворих політик доступу до критичних ресурсів та використання двофакторної аутентифікації для підвищення рівня безпеки. Іншим важливим аспектом є налаштування міжмережевих екранів та систем виявлення вторгнень, які можуть моніторити мережевий трафік і блокувати потенційно небезпечні дії.

Для забезпечення максимального рівня безпеки важливо також проводити регулярні аудити системи та тестування проникнення, які допоможуть виявити потенційні загрози та вжити відповідних заходів для їх нейтралізації. Це особливо актуально в умовах, коли кіберзагрози постійно змінюються і з'являються нові методи атак. Завдяки цьому з використанням платформи TryHackMe отримують не тільки знання про існуючі вразливості, а й розуміння того, як підтримувати безпеку в умовах постійних змін.

Віртуальні машини на платформі TryHackMe є незамінним інструментом для підготовки фахівців у галузі кібербезпеки. Вони дозволяють безпечно експериментувати з різними методами атак, вивчати сучасні засоби захисту та розробляти нові стратегії для забезпечення інформаційної безпеки. Завдяки цим практичним навичкам студенти мають можливість краще розуміти реалії сучасної кібербезпеки, що робить їх готовими до роботи у справжніх умовах. Платформа допомагає розвивати критичне мислення, вміння аналізувати загрози та створювати ефективні заходи захисту, що є необхідними для побудови надійної системи інформаційної безпеки у сучасному цифровому світі.

Загалом, навчання на платформі TryHackMe сприяє формуванню нової генерації фахівців з кібербезпеки, які не тільки розуміють сучасні загрози, але й здатні ефективно протидіяти їм. Це забезпечує більшу безпеку для організацій, компаній та державних структур, що покладаються на захищеність інформаційних систем.

Висновки. Платформа TryHackMe є інструментом як для самостійного навчання кібербезпеці, так і для проведення наукових досліджень в цій галу-

зі. Її переваги полягають у систематичному підході до навчання, практичній орієнтації, актуальності контенту та гнучкості використання.

Інформаційні джерела

1. Ящук В. І. Моніторинг процесів функціонування інформаційно-комунікаційних систем. ITSec: Безпека інформаційних технологій: матеріали XIII Міжнар. наук.-техн. конф., м. Львів, 9–11 трав. 2024 р. Л.: ЛНУ ім. І. Франка, 2024, 257 с. С. 253–254.

2. Рошинець І., Ящук В., Федина Б. Актуальність використання віртуальних та хмарних технологій. Інформаційна безпека та інформаційні технології: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – Львів: Растр-7, 2022. – 380 с. С. 133–136.

3. Ящук В. І. Методика забезпечення безпеки інформаційних систем та реагування на кіберінциденти кібербезпековими центрами. Scientific Collection "InterConf+", 45(201): with the Proceedings of the 8thInternational Scientific and Practical Conference "International Scientific Discussion: Problems, Tasks and Prospects" (May 19–20, 2024; Brighton, United Kingdom)/ comp. by LLC SPC "InterConf". Brighton: A.C.M. Webb Publishing Co Ltd., 2024. 678 p. pp. 632–641.

УДК 621.391:629.783:004.056.5

МОДЕЛЬ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ЗВ'ЯЗКУ З ОРБІТАЛЬНИМИ НАНОСУПУТНИКАМИ

Олександр ЛЮБІМОВ
Іван ІОВЕНКО
Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут", м. Харків, Україна.

Abstract. *The issue of organizing secure communication for nanosatellites has become increasingly relevant due to the rapid growth of the industry, especially considering the limited resources. The main challenges include ensuring data transmission security, and protection against spoofing and cyber threats. The solution lies in implementing hardware encryption modules, lightweight cryptographic algorithms, and key management systems adapted to space conditions.*

Keywords: *nanosatellites, information protection, communication protection, encryption.*

Анотація. *Питання огляду організації захищеного зв'язку для наносупутників стало ще більш актуальним через швидке зростання індустрії, особливо з огляду на обмежені ресурси. Основні проблеми включають забезпечення безпеки передачі даних, захист від спуфінгу та кіберзагроз. Рішенням є впровадження апаратних модулів шифрування, легких криптографічних алгоритмів та систем управління ключами, адаптованих до умов космосу.*

Ключові слова: *наносупутник, захист інформації, захист зв'язку, шифрування.*

Вступ. Стрімке зростання індустрії малих супутників призвело до поширення наносупутників – компактних космічних апаратів вагою менше 10 кілограмів [1]. Зі свого започаткування в 1999 році, наносупутники створили справжній прорив та станом на кінець 2023 року, було виведено майже 2800 наносупутників. Хоча ці мініатюрні супутники мають численні переваги, такі як зниження вартості і скорочення термінів розробки, вони створюють унікальні виклики, коли йдеться про забезпечення безпечної передачі даних між супутником і наземними станціями.

Збереження конфіденційності, цілісності та доступності даних, якими обмінюються наносупутники на орбіті та їхні наземні аналоги, є критично важливим завданням. Наносупутники мають жорсткі обмеження за розміром, вагою і енергоспоживанням, що залишає мало місця для спеціального обладнання і програмного забезпечення для забезпечення безпеки. Це ускладнює впровадження надійних алгоритмів шифрування і систем управління ключами, здатних протистояти суворим умовам космічного середовища.

На додаток до ресурсних обмежень, наносупутники вразливі до інших загроз у безпеці. Лінії передачі даних між супутником і наземною станцією повинні бути захищені від потенційного прослуховування і перехоплення сигналу несанкціонованими сторонами. Переривчастий характер вікон зв'язку, зумовлений динамікою орбіти і покриттям наземної станції, також може ускладнити процеси обміну ключами і аутентифікації, необхідні для безпечної передачі даних. Крім того, наносупутники можуть бути вразливими до віддалених програмних атак, які можуть порушити цілісність бортових механізмів безпеки.

Щоб вирішити ці проблеми, дослідники та інженери вивчають різноманітні методи і протоколи безпеки, пристосовані до унікальних обмежень наносупутникових систем. Серед них – використання легких алгоритмів шифрування, таких як ChaCha20-Poly1305 або AES-GCM, які забезпечують надійну конфіденційність і цілісність даних, не перевантажуючи ресурси супутника [2]. Криптографія еліптичних кривих (ECC) пропонує альтернативу традиційній криптографії з відкритим ключем, забезпечуючи порівнянну безпеку при значно менших розмірах ключів, що робить її більш придатною для наносупутників з обмеженими ресурсами.

На додаток до криптографічних рішень, такі технології, як безпечне завантаження і перевірка цілісності прошивки, можуть допомогти захистити наносупутники від несанкціонованих модифікацій і програмних атак. Інноваційні схеми управління ключами, такі як попередньо розподілені ключі або криптографія на основі ідентифікації, можуть спростити процес обміну і розподілу ключів для наносупутників з переривчастим зв'язком. Нарешті, використовуючи більші обчислювальні ресурси і надійний зв'язок наземних станцій, можна впровадити системи моніторингу безпеки і виявлення аномалій, що підвищить загальний рівень безпеки мережі зв'язку між наносупутниками і наземними станціями.

Проблема: Більшість наносупутників будується на так званих COTS

(Commercial off the shelf) [3] компонентах, що комерційно доступні, тобто можуть бути придбані як готові вироби. Більшість цих виробів є достатньо простими розробками, основною метою яких є забезпечення обчислювальної потужності при мінімізації споживаної енергії.

Україна на сьогодні мала 8 пусків малих та наносупутників з яких тільки 2 видались вдалими. 2 останніх пуски були невдалими, зокрема супутник "Січ-2–30" та супутник КПІ – PolyItan-HP-30. Офіційною версією втрати є проблеми з надійним зв'язком та системою енергозабезпечення, а також надлишкове інформаційне навантаження, що в термінах кібербезпеки має назву "спуфінгу" (від. Англ. Spoof).

Частиною проблеми захищеності є бажання знизити енергоспоживання супутника шляхом використання більш простих процесорів з обмеженою швидкодією. Це у свій час унеможливлює використання таких процесорів для шифрування та дешифрування в реальному часі.

У такому випадку *проблему досліду* можливо сформулювати як бажання отримати надійне та просте шифрування інформації наносупутнику яка використовується як телеметрія та дані корисного навантаження. *Вторинним завданням* є бажання отримати захист від спуфінгу.

Методи рішення: Першим методом рішення проблеми є впровадження спеціалізованих апаратних модулів для шифрування, які працюють незалежно від основного процесора. Такі модулі можуть використовуватися для забезпечення шифрування даних корисного навантаження в реальному часі, що значно знижує ризики кібератак, зокрема спуфінгу в контексті захисту процесу оновлення вбудованого програмного забезпечення. Завдяки шифруванню оновлень, забезпечується перевірка цілісності та автентичності програмних пакетів, що унеможливлює установку шкідливих або модифікованих файлів. Використання інтегральних схем шифрування (криптопроцессорів) не тільки знижує навантаження на центральний процесор, алей і підвищує загальний рівень безпеки.

Типовим на сьогодні є використання так званих "довірених модулів платформи" – Trusted Platform Module (рис. 1).

Таке рішення надає можливість автономно (незалежно від мікропроцесору) виконувати наступні операції:

– надійне та захищене зберігання приватних ключів;

– оновлення ключів;

– автомат швидкого шифрування та дешифрування інформації за найбільш-розповсюдженими алгоритмами (RSA-4096, AES-128, AES-192, AES-256, ECC NIST P384, SHA2-384);

– генератор випадкових чисел класу NIST;

– надання унікального ідентифікатору;

– енергонезалежна пам'ять для зберігання відкритого ключу та інших налаштувань безпеки для встановлення первинного сеансу зв'язку;

– допоміжні функції керування інформацією та/або зовнішніми електронними схемами.

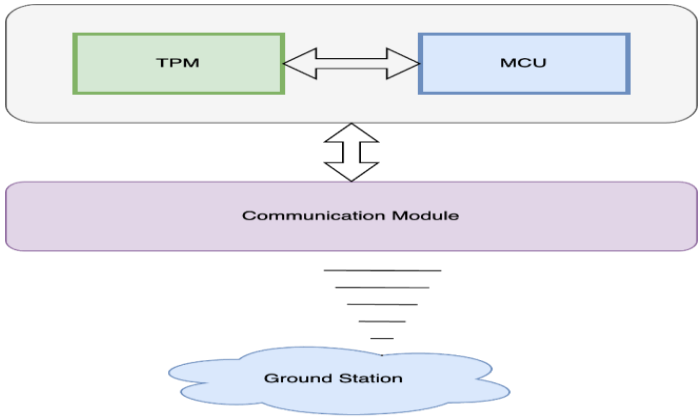


Рисунок 1 – Типова схема використання модуля “довіреної платформи” – TPM

Ще одним перспективним методом вирішення проблеми є використання програмованих логічних інтегральних схем (FPGA), які дозволяють реалізувати криптографічні алгоритми без значного збільшення споживання. FPGA забезпечують можливості налаштовувати шифрувальні алгоритми під конкретні вимоги проєкту, що дозволяє досягати високої продуктивності навіть на обмежених апаратних ресурсах. *Наприклад*, реалізація алгоритмів симетричного шифрування, таких як AES (Advanced Encryption Standard), на FPGA дозволяє забезпечити швидке та надійне шифрування, що є особливо важливим для передачі даних наносупутників в умовах обмежених енергетичних можливостей. Найбільшою проблемою використання FPGA є необхідність володіти певними навичками програмування на мові Verilog/VHDL та високий кошторис таких інтегральних схем.

Також рішенням може бути використання спеціалізованих модулів безпеки, відомих як HSM (Hardware Security Module), які виконують криптографічні операції в ізольованому середовищі. HSM можуть також виконувати функції надання доказів втручання та ведення журналу та сповіщень безпекових питань. Такі модулі також дозволяють прискорювати процеси шифрування та дешифрування даних, що знижує навантаження на основний процесор і дозволяє оптимізувати роботу всього наносупутника. Такі модулі є аналогами модулів TPM але зазвичай мають більшу вбудовану енергонезалежну пам’ять для зберігання журналу подій.

Додатковим рішенням може бути використання мікроконтролерів із вбудованими криптографічними акселераторами. Такі рішення забезпечують високий рівень безпеки при мінімальному енергоспоживанні, що є важливим для наносупутників. Ці мікроконтролери здатні виконувати складні криптографічні алгоритми з мінімальним впливом на загальну продуктив-

ність системи, що дозволяє значно підвищити ефективність роботи супутника в умовах низької енергоефективності. В останні роки такі мікроконтролери стали достатньо поширеними, але їх основною проблемою є відсутність алгоритмів завантаження ключів, їх зміна та видалення, що створює додаткові вимоги до розробника таких систем. Вимоги до крипто-стійкості систем які дотичні до використання у наносупутниках потребують значного часу від розробника вбудованого ПЗ.

***Рішення*:** Рішенням проблеми є використання зовнішніх електронних підсистем та модулів шифрування та дешифрування інформації, а саме інтегральних схем класу TPM.

Зазвичай такі підсистеми представлені електронними інтегральними схемами які дозволяють виконувати шифрування інформації з мінімальним втручанням центрального процесору. Єдиним завданням центрального процесору у такому випадку є передавання та прийом шифрованого та дешифрованого трафіку. У наносупутнику що розробляється командою ХАІ, та його авторському обчислювачі “Боривітер” [4] пропонується використання TPM Infineon TPM Optiga SLB 9673 (рис. 2).

Рисунок 2 – Інтегральна мікросхема “довіреного модуля платформи” – Infineon Optiga TPM, SLB 9673

Використання рішення на TPM SLB 9673 дозволяє вирішити наступні завдання:

– шифрування та дешифрування інформації без завантаження центрального обчислювального мікроконтролеру;

– шифрування у відповідності до CCSDS протоколу, що використовується у стандартних підходах передачі інформації на наземні станції та є офіційним протоколом Європейського Космічного Агенства (ESA, European Space Agency);

– спрощує отримання відповідності вимогам NIST/NIST2;

– надає можливість відповідати вимогам NIST SP 800-53 (space system security controls);

– дозволяє реалізувати спрощений механізм знаходження та корекції помилок – EDAC (Error Detection And Correction), який зазвичай використовується для контролю космічної радіації на НОЗ та в поясі Алана;

– дозволяє прискорити та спросити механізм тестування бортових запам'ятовуючих пристроїв при старті (тест включення);

– дозволяє зекономити ПЗП та ОЗП потрібне для реалізації вищезазначених алгоритмів засобами мікроконтролеру.

Типовим використанням зовнішнього модуля довіреної платформи для шифрування або дешифрування інформації за допомогою AES-256-CBC буде наступна діаграма послідовності (рис. 3).

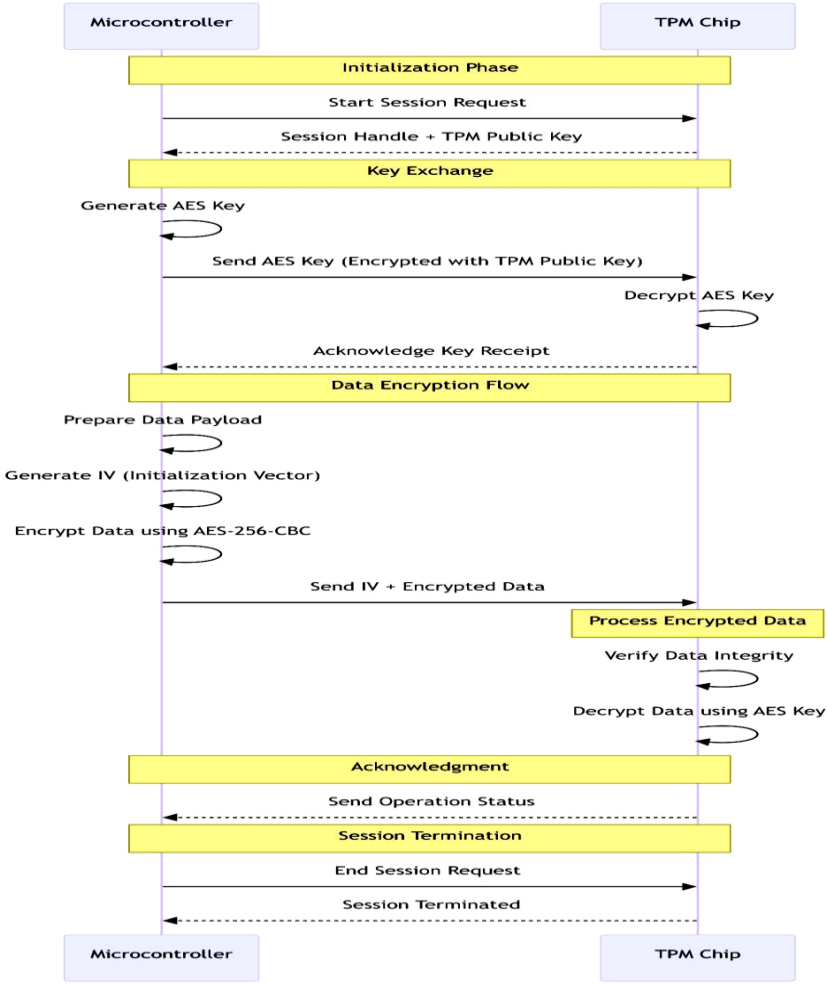


Рисунок 3 – UML діаграма послідовності, реалізація шифрування за допомогою AES-256-CBC в парі мікроконтролер + TPM модуль

Висновки. Сучасні модулі класу TPM є дієвим, енерго- та обчислювально-ефективним рішенням як щодо завдань класичного шифрування та дешифрування інформації, так і для завдань допоміжного характеру – перевірку цілісності пакетів даних, прискорення тестування пам'яті. Використання рішень TPM дозволяє створювати програмно-апаратні рішення для бортових обчислювачів наносупутників з урахуванням складності, часових обмежень та вимог до енергоефективності та надійності.

Дослідження з пошуку надійного та стійкого рішення з криптозахисту каналів зв'язку між ЛА або КА та наземною станцією, було виконано при підтримці та в рамках гранту НФДУ: №2023.04/0143 "Експериментальне відпрацювання бортового обчислювача безпілотного літального апарата подвійного призначення".

Інформаційні джерела

1. Martin n. Sweeting. Modern small satellites-changing the economics of space // Proceedings of the IEEE. – 2018. – vol. 106. – ISSUE 3, pp. 343–361. doi: 10.1109/JPROC.2018.2806218.

2. Amr zeedan, tamer khattab. Cubesat communication subsystems: a review of on-board transceiver architectures, protocols, and performance // IEEE ACCESS. – 2023. – vol. 11, pp. 88161–88183. doi: 10.1109/ACCESS. 2023.3304419.

3. Liubimov O. and Liubimov M. (2023) "USE of open-source cots/mots hardware and software platforms for the build up of the cubesat nanosatellites", journal of rocket-space technology, 31(4), pp. 138–147. doi: 10.15421/452318.

4. Офіційний сайт розробників бортового обчислювача "Боривітер" – Фалко Інжинірінг. URL: https://www.falco.engineering/ (дата звернення: 17.11.2024).

УДК 004.056.5

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДИК ФОРМУВАННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

Денис ОСТАПЕЦЬ
Олексій СУХОМЛИН
Український державний університет науки і технологій, м. Дніпро, Україна.

Abstract. *The study examines modern methodologies for forming functional security profiles (FSP) of information. Key requirements for the methodologies are identified, and their advantages and disadvantages are analyzed. Recommendations for optimizing FSP formation processes are proposed, including the automation of verification processes for formed FSPs and the use of intelligent methods.*

Keywords: *functional security profile, information security, automated system, intelligent methods.*

Анотація. *В роботі розглянуто сучасні методики щодо формування функціональних профілів захищеності (ФПЗ) інформації. Визначено ключові вимоги до методик, проаналізовано їх переваги та недоліки. Запропоновано рекомендації з оптимізації процесів формування ФПЗ, зокрема через автоматизацію процесів верифікації сформованою ФПЗ та за рахунок використання інтелектуальних методів.*

Ключові слова: *функціональний профіль захищеності, інформаційна безпека, автоматизована система, інтелектуальні методи.*

Сучасний розвиток цифрових технологій супроводжується зростанням загроз інформаційній безпеці, що робить захист інформації одним із найважливіших завдань. Важливою складовою ефективного захисту є розробка функціональних профілів захищеності (ФПЗ), які визначають набір заходів для запобігання несанкціонованому доступу. Вибір оптимальної методики формування ФПЗ має ключове значення, оскільки впливає на ефективність захисту, витрати часу та ресурсів.

Метою дослідження є аналіз існуючих методик формування ФПЗ, їх переваг і недоліків, а також визначення шляхів покращення процесів формування профілів. Досягнення цієї мети передбачає: визначення основних вимог до методик формування ФПЗ, аналіз і порівняння сучасних підходів, розробку рекомендацій щодо оптимізації процесів формування ФПЗ.

Основні вимоги до методик формування ФПЗ можна сформулювати так:

Часова ефективність – методика повинна забезпечувати мінімальні витрати часу на формування ФПЗ без втрати якості.

Важливою є *можливість скорочення часу* за рахунок автоматизації процесів.

Зрозумілість і простота впровадження – методика повинна бути зрозумілою для фахівців із різним рівнем підготовки. Мінімізація складності допомагає знизити ризики помилок при формуванні ФПЗ.

Незалежність від людського фактора – зменшення залежності результатів від кваліфікації експертів шляхом стандартизації процедур і використання допоміжних інструментів (*наприклад*, опитувальних таблиць або алгоритмів самоперевірки).

Гнучкість та адаптивність – методика має враховувати можливість створення нестандартних профілів, що відповідають специфічним потребам інформаційної системи.

У дослідженні здійснено аналіз низки методик формування ФПЗ, їх оцінка проведена на основі визначених вимог:

Стандартний вибір ФПЗ [1] – методика забезпечує низьку часову ефективність через необхідність ретельного аналізу середовища та обрати ФПЗ зі стандартних, який найбільше відповідає заданим вимогам. Середньої складності, навіть для менш досвідчених фахівців, завдяки використанню готових рішень. Висока залежність від кваліфікації експерта через необхідність аналізу середовища і вибору найбільш відповідного профілю. Обмежена гнучкість, методика орієнтована виключно на вибір із готових шаблонів.

Методика опитувальних таблиць [2] – часові витрати середні, оскільки таблиці полегшують процес систематизації, проте етап верифікації може бути ресурсозатратним. Методика середня по складності, у використанні. Вимагає базових знань у сфері безпеки для ефективної верифікації профілю. Помірна залежність від людського фактору, оскільки таблиці частково стандартизують процес. Однак якість результату залежить від експертної оцінки. Висока гнучкість, дозволяє створювати нестандартні профілі та адаптувати їх до специфічних вимог.

Ймовірнісно-вартісна методика [3] – потребує значного часу через необхідність математичних розрахунків, зокрема оцінки ймовірностей загроз та економічної ефективності захисних заходів. Високий рівень складності через необхідність математичного моделювання. Підходить лише для досвідчених фахівців. Висока залежність, адже експерти визначають ймовірності загроз і ключові параметри моделей. Висока гнучкість, оскільки методика враховує економічні обмеження та дозволяє створювати адаптовані профілі.

Логіко-матричний метод [4] – часова ефективність середня, оскільки методика дозволяє автоматизувати вибір профілів після початкової побудови матриць. Середній рівень складності. Побудова матриць знань, може бути складною для новачків, та вимагає високої кваліфікації експерта, проте сам процес використання зрозумілий. Помірна гнучкість. Метод орієнтований на стандартні ФПЗ, але його можна адаптувати для створення нових профілів за потреби.

Адаптивний метод [5] – методика демонструє середню часову ефективність, оскільки автоматизація процесів частково компенсує складність математичних обчислень. Складний для впровадження через використання математичних оптимізаційних моделей. Вимагає глибоких знань як у галузі безпеки, так і в математичному моделюванні. Висока гнучкість.

Аналіз показує, що жодна з методик не відповідає одночасно всім вимогам на найвищому рівні. Стандартний вибір ФПЗ є найпростішим для розуміння, але потребує щільного аналізу середовища, також присутнє обмеженя у гнучкості. Опитувальні таблиці є компромісним варіантом, забезпечуючи гнучкість і відносну простоту. Ймовірнісно-вартісний та адаптивний методи є найбільш гнучкими, через кількість враховуємих параметрів але складними і залежними від експертів. Логіко-матричний також не відрізняється високою часовою ефективністю, а також кваліфікація експерта грає визначну роль в ефективності обраної ФПЗ.

Вирішити наведені проблеми можна, завдяки впровадження програмних інструментів для генерації та верифікації ФПЗ, які знижують вплив людського фактору. Використання інтелектуальних методів, може значно підвищити ефективність формування ФПЗ, за рахунок зменьшення впливу суб'єктивної експертної оцінки на сформований ФПЗ в результаті процесу проектування захищеної АС.

Висновки. Аналіз існуючих методик показав, що оптимізація процесів можлива через впровадження програмних інструментів для генерації та вери-

фікації ФПЗ, а також через впровадження інтелектуальних методів, що полегшать процес формування ФПЗ при проектуванні систем захисту інформації.

Інформаційні джерела

1. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. URL: http://www.dstszi.gov.ua/dstszi/ doccatalog/

2. Лєншин А. В., Буслов П. В. Метод формування функціональних профілів захищеності від несанкціонованого доступу // Радіоелектронні і комп'ютерні системи : науч. тр. – Х.: Нац. аэрокосм. ун-т "ХАИ", 2010. – Вып. 7(48). – С. 77–81. – URL: http://nbuv.gov.ua/UJRN/recs_2010_7_15

3. Ткач Ю. М. Метод вибору функціонального профілю захищеності // Інформатика та математичні методи в моделюванні. – 2020. Т. 10, № 1–2. – С. 68–74.

4. Юдін О. К., Бучик С. С., Мельник С. В. Теоретичні основи визначення стандартних функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу. Наукоємні технології. 2016. Вип. 2. – С. 195–205.

5. Потенко О. С. Методи визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз: автореф. дис. канд. техн. наук : 05.13.21. Київ, 2024. – 24 с.

УДК 004.056.5

МОЖЛИВОСТІ ВИКОРИСТАННЯ ДОКАЗІВ НУЛЬОВОГО РОЗГОЛОШЕННЯ У СИСТЕМАХ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Денис ОСТАПЕЦЬ
Володимир МОТИЛЕНКО
Український державний університет науки і технологій, м. Дніпро, Україна.

Abstract. *The study examines the potential of zero-knowledge proofs (ZKP) in electronic voting systems. ZKPs ensure anonymity, verifiability, receipt-freeness, and resistance to manipulation. Technologies such as zk-SNARK and zk-STARK are analyzed, highlighting their advantages and limitations. The importance of trust in the voting server is emphasized for implementing certain principles of electronic voting systems.*

Keywords: *e-voting, zero-knowledge, cryptography.*

Анотація. *В роботі розглядаються можливості застосування доказів із нульовим розголошенням (ZKP) у системах електронного голосування. ZKP забезпечують анонімність, перевіряємість, відсутність квитанцій і стійкість до маніпуляцій. Проаналізовано технології zk-SNARK і zk-STARK, їх переваги та недоліки. Відзначено важливість довіри до серверу для реалізації деяких принципів систем електронного голосування.*

Ключові слова: *електронне голосування, докази нульового розголошення, криптографія.*

Однією з ключових проблем електронного голосування (ЕГ) є забезпечення конфіденційності виборців і надійності процесу. Сучасні криптографічні підходи дозволяють передивитися методи побудови таких систем.

Метою дослідження є аналіз можливостей застосування доказів з нульовим розголошенням (ZKP) у системах електронного голосування для забезпечення анонімності, автентичності голосів і прозорості підрахунку. Основними завданнями є побудова структури системи електронного голосування на основі ZKP, визначення властивостей ZKP для подальшого порівняння їх з іншими можливими методами побудови систем ЕГ.

Основними властивостями які доцільно зазначити у якості вимог до системи ЕГ [1] є анонімність голосування, стійкість системи до поведінки зловмисника (надійність), можливість перевірки правильності підрахунку (універсальна перевіряємість), відсутність квитанцій, а також те, що часткові результати не повинні бути опубліковані (чесність).

У роботі виконано аналіз сучасних криптографічних протоколів, зокрема zk-SNARK і zk-STARK, а також порівняльний аналіз їх властивостей у контексті застосування до електронного голосування.

Процес голосування з використанням доказів нульового розголошення поділяється на декілька етапів:

– на першому етапі кандидати та голосуючі реєструються в системі, для цього адміністратори системи повинні авторизувати ідентифікатор голосуючих, а також внести кандидатів в список кандидатів на сервері електронного голосування;

– на другому етапі у голосуючих є можливість згенерувати бюлетень, та сформувати доказ того що вони дотримуються правил голосування (їх ідентифікатор валідний, кандидат знаходиться у списку, це перший голос голосуючого);

– на третьому етапі сервер робить підрахунок голосів і повідомляє результати.

Перший етап є доволі узагальнений для будь-якої системи електронного голосування і не є унікальним для системи на базі доказів нульового розголошення. Третій етап більше відноситься до інфраструктурних питань і теж лежить поза межами систем на базі доказів нульового розголошення. Тому, у даній роботі, аналіз сфокусований на другому етапі.

У системах ЕГ на базі доказів нульового розголошення (рис. 1) бюлетень та доказ є невід'ємною частиною. Ті, хто голосує, формують бюлетень з доказом для відправки серверу.

Сервер перевіряє відповідність правилам і приймає голос. За таймером сервер може опрацювати голоси і оприлюднити результат. Разом з результатом сервер може опублікувати докази для того, щоб аудитори могли перевірити правильність підрахунку голосів. У результаті цього процесу ідентифікатор користувача не фігурує у бюлетені-доказі а тому зберігається анонімність глосуючого.

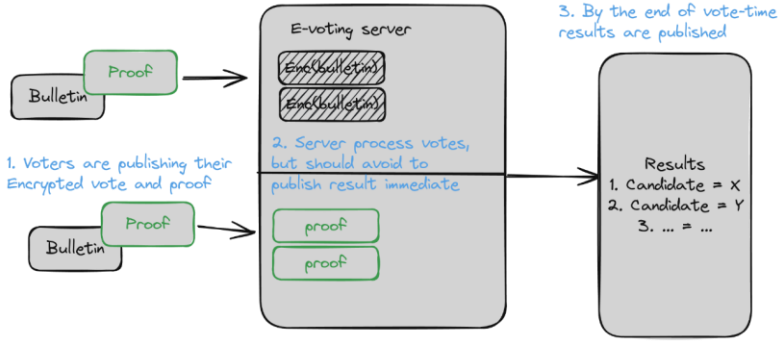


Рисунок 1 – Спрощена структура збору голосів у системі ЕГ на базі доказів нульового розголошення

Загалом, докази з нульовим розголошенням дозволяють перевіряти коректність голосів без розкриття їхнього змісту. Система на базі ZKP гарантує, що:

1. Анонімність голосування зберігається, оскільки усі голоси шифруються на стороні відправника.
2. Універсальна перевіряємість забезпечується через можливість повторного підрахунку голосів, що залишаються у зашифрованому вигляді.
3. Відсутність квитанцій виключає можливість доведення виборцем факту свого голосу, що унеможливлює зовнішній тиск.

Надійність досягається за рахунок автентифікації виборця та фільтрації небажаних голосів.Докази з нульовим розголошенням є ефективним засобом підвищення безпеки та прозорості електронного голосування. Вони дозволяють створювати системи, що задовольняють основні вимоги до голосування, зокрема анонімність, перевіряємість і захист від маніпуляцій.

Технології zk-SNARK і zk-STARK [2, 3] є більш універсальні ніж гомоморфне шифрування, оскільки дозволяють не інтерактивно провести операції на зашифрованих даних, а також довести, що зашифровані данні знаходяться у необхідному діапазоні. Що робить їх привабливими для впровадження у системи електронного голосування. Проте реалізація вимоги чесності залежить від рівня довіри до серверу голосування, що виходить за рамки технічного підходу ZKP.

Висновки. Докази з нульовим розголошенням є ефективним засобом підвищення безпеки та прозорості електронного голосування. Вони дозволяють створювати системи, що задовольняють основні вимоги до голосування, зокрема анонімність, перевіряємість і захист від маніпуляцій.

Інформаційні джерела

1. Liaw H.-T. A secure electronic voting protocol for general elections. Computers & Security. 2004. Vol. 23, no. 2, pp. 107–119.

2. Panait A.-E. F., Olimid R. On Using zk-SNARKs and zk-STARKs in Blockchain-Based Identity Management // Innovative Security Solutions for Information Technology and Communications. 2020. T. 12596. URL: https://link.springer.com/chapter/10.1007/978-3-030-69255-1_9.

3. Ashur T., Dhooghe S. MARVELlous: a STARK-friendly family of cryptographic primitives // International Association for Cryptologic Research. 2018. No. 1098. URL: https://eprint.iacr.org/2018/1098.

УДК 004.056.5

АНТИВІРУСНІ ПРОГРАМИ:ЇХ ЗНАЧЕННЯ ТА ЕФЕКТИВНІСТЬ У ЗАХИСТІ ДАНИХ

Ілля КУРІННИЙ
Віталій СВІТЛИЧНИЙ
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The role of antivirus software in ensuring cybersecurity and protecting data from modern threats is examined. The main types of malicious software and antivirus functions, such as real-time protection, blocking phishing attacks and ransomware, are described. The advantages of popular antivirus solutions and their additional tools are analyzed. The importance of antiviruses as a key element in a comprehensive protection system is highlighted.*

Keywords: *antivirus software, cybersecurity, phishing attacks, ransomware, data protection, Kaspersky, Avast, ESET NOD32, McAfee.*

Анотація. *Розглянуто роль антивірусного програмного забезпечення у забезпеченні кібербезпеки та захисті даних від сучасних загроз. Описуються основні види шкідливого програмного забезпечення та функції антивірусів, такі як захист у реальному часі, блокування фішингових атак та програм-вимагачів. Аналізуються переваги популярних антивірусних рішень та їхні додаткові інструменти. Висвітлюється важливість антивірусів як ключового елемента у системі комплексного захисту.*

Ключові слова: *антивірусне програмне забезпечення, кібербезпека, фішингові атаки, програми-вимагачі, захист даних, Kaspersky, Avast, ESET NOD32, McAfee.*

Антивірусне програмне забезпечення – це спеціалізована програма, призначена для виявлення, запобігання та видалення зловмисного програмного забезпечення, широко відомого як зловмисне програмне забезпечення. Він діє як воротар для ваших цифрових пристроїв, контролюючи дані та блокуючи потенційні загрози від заподіяння шкоди. Його основною функцією є захист комп'ютерів і мобільних пристроїв від шкідливих програм, таких як віруси, черв'яки, трояни, програми-вимагачі та шпигунські програми [1].

Антивірус також забезпечує захист від небезпечних вебсайтів і електронних листів, які можуть містити віруси або інші загрози. Це допомагає

запобігти крадіжці особистих даних, таких як паролі, банківські реквізити та номери кредитних карток.

В інтернеті існує безліч видів вірусних загроз. Ідеальний антивірус повинен забезпечувати захист від усіх них. Серед найпоширеніших загроз – віруси, які додають шкідливий код в програми; черв'яки, що поширюються через мережі; програми-шпигуни, які збирають конфіденційну інформацію; трояни, що виконують приховані дії; фішингові програми, які крадуть особисті дані; віруси-шифрувальники, що блокують доступ до файлів; та майнери, які використовують ресурси пристрою для видобутку криптовалют. Крім того, існують більш складні загрози, такі як руткіти, що приховують вірусну активність, hoax-програми, які вводять користувача в оману, та ботнети, що використовують заражені пристрої для проведення масштабних атак [2].

Кібератаки можуть призвести до втрати важливих даних. *Наприклад*, програми-вимагачі шифрують файли та вимагають викуп за їх розшифровку. Використання антивірусного програмного забезпечення допомагає запобігти таким атакам і забезпечити захист особистої та робочої інформації. Відновлення даних після атаки може бути дорогим і, у деяких випадках, неможливим, що робить превентивні заходи особливо важливими [4].

Надійні антивірусні програми забезпечують безпеку під час роботи в Інтернеті, пропонуючи розширення для популярних веб-браузерів. Такі розширення перевіряють веб-сторінки, завантаження та електронні листи на наявність шкідливих файлів і вкладень. Антивірус також підвищує безпеку онлайн-платежів, попереджаючи користувачів про підроблені платіжні портали, які можуть використовуватись у фішингових атаках [3].

Таблиця 1.

Аналізу сервісів та інструментів антивірусних програм для захисту даних

Характеристика	*Kaspersky*	*Avast*	*ESET NOD32*	*McAfee*
Платні функції	так	так	так	так
Захист у реальному часі	так	так	так	так
Блокування фішингових атак	так	так	так	так
Захист від програм-вимагачів	так	так	так	так
Автоматичне оновлення баз вірусів	так	так	так	так
Додаткові інструменти (VPN, менеджер паролів)	так	так	ні	так
Сумісність із платформами	Windows, Mac, Android, iOS	Windows, Mac, Android, iOS	Windows, Mac, Android	Windows, Mac, Android, iOS
Кількість користувачів	400 млн+	435 млн+	110 млн+	600 млн+

Висновки. Про важливість та ефективність антивірусних програм свідчать про їхню ключову роль у сучасному світі кібербезпеки. Антивірусне програмне забезпечення допомагає захистити користувачів від різноманітних шкідливих програм і загроз, забезпечуючи безпеку особистих та професійних даних. Воно виконує не тільки функцію виявлення і нейтралізації загроз, але й запобігає потенційним кіберзлочинам, таким як крадіжка особистої інформації та фішингові атаки.

Незважаючи на високу ефективність антивірусних рішень, варто пам'ятати, що вони є лише одним із елементів комплексного підходу до кіберзахисту. Регулярні оновлення, свідоме використання Інтернету, дотримання базових правил цифрової гігієни та додаткові заходи безпеки допоможуть значно знизити ризики. Тому антивірусне програмне забезпечення має залишатися обов'язковою частиною захисних заходів для всіх, хто прагне убезпечити свою інформацію від кібератак.

Інформаційні джерела

1. What is Antivirus Software? URL: https://www.timusnetworks.com/what-is-antivirus-software/ (дата звернення 13.11.2024).

2. Навіщо потрібні антивіруси? https://itez.com.ua/why-do-you-need-antivirus.html (дата звернення 13.11.2024).

3. Essential Benefits Of Antivirus Software. URL: https://geekflare.com/ cybersecurity/ advantages-using-antivirus/ (дата звернення 13.11.2024).

4. Why Is It Important to Install an Antivirus Program? URL: https:// infocons.org/blog/2024/07/29/why-is-it-important-to-install-an-antivirus-program/ (дата звернення 13.11.2024).

УДК 004.838

ЗАХИСТ СИСТЕМ УПРАВЛІННЯ ПРОМИСЛОВИМИ ПРОЦЕСАМИ (SCADA)

Василь ЛУЧИК
Назар ПРОКОПЧУК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *Supervisory control and data acquisition (SCADA) systems are a key element of modern production and infrastructure, providing real-time monitoring and control of technological processes. They are widely used in industries such as energy, water supply, transportation, oil and gas, and manufacturing. The main functions of SCADA include data collection, processing, archiving, process visualization, as well as operational management and response to malfunctions. In the context of digitalization, SCADA systems become vulnerable to cyber threats, which requires the implementation of*

effective protection strategies such as network segmentation, access control, encryption, threat monitoring, software updates, and personnel training. Given their importance for critical infrastructures, SCADA protection is a priority to ensure stable and secure operation of industrial processes.

Keywords: *SCADA, industrial process control systems, cybersecurity, monitoring, automation, critical infrastructure, cyber threats, network segmentation, encryption, access control, personnel training.*

Анотація. *Системи управління промисловими процесами (SCADA) є ключовим елементом сучасного виробництва та інфраструктури, забезпечуючи моніторинг і управління технологічними процесами в реальному часі. Вони знаходять широке застосування у таких галузях, як енергетика, водопостачання, транспорт, нафтогазова промисловість і виробництво. Основні функції SCADA включають збір даних, їх обробку, архівування, візуалізацію процесів, а також оперативне управління і реагування на несправності. В умовах цифровізації SCADA-системи стають вразливими до кіберзагроз, що вимагає впровадження ефективних стратегій захисту, таких як сегментація мережі, контроль доступу, шифрування, моніторинг загроз, оновлення програмного забезпечення та навчання персоналу. Зважаючи на їхнє значення для критично важливих інфраструктур, захист SCADA є пріоритетом для забезпечення стабільної та безпечної роботи промислових процесів.*

Ключові слова: *SCADA, системи управління промисловими процесами, кібербезпека, моніторинг, автоматизація, критична інфраструктура, кіберзагрози, сегментація мережі, шифрування, управління доступом, навчання персоналу.*

Системи управління промисловими процесами (SCADA) відіграють ключову роль у сучасному виробництві та інфраструктурі, забезпечуючи моніторинг і контроль за різними технологічними процесами в реальному часі. Вони використовуються в таких галузях, як енергетика, водопостачання, транспорт і виробництво, роблячи ці системи критично важливими для функціонування економіки та безпеки суспільства. Однак розвиток технологій і підвищення рівня цифровізації призводять до збільшення кіберзагроз і ризиків, пов’язаних із безпекою SCADA. Це вимагає застосування надійних стратегій і рішень для захисту систем від несанкціонованого доступу, кібератак та інших потенційних загроз. Вступ до вивчення аспектів захисту SCADA є важливим для розуміння способів захисту цих систем та забезпечення стабільної та безпечної роботи промислових процесів.

SCADA (Supervisory Control And Data Acquisition – диспетчерське управління і збір даних) – це програмний комплекс, що забезпечує розробку та функціонування систем для збору, обробки, відображення та архівування інформації про об’єкт моніторингу чи управління в реальному часі. SCADA може бути частиною автоматизованих систем керування технологічними процесами (АСК ТП), систем обліку електроенергії (АСКОЕ), екологічного моніторингу, автоматизації будівель, проведення наукових експериментів тощо. SCADA-системи використовуються у різних галузях, де необхідно забезпечити операторський контроль технологічних процесів у режимі реа-

льного часу. Таке програмне забезпечення встановлюється на комп'ютерах і для зв'язку з об'єктами використовує драйвери введення-виведення або сервери OPC/DDE. Програмний код може бути створений вручну або згенерований у середовищі проектування. Деякі SCADA-системи доповнюються додатковими програмами для програмування промислових контролерів, і такі системи називаються інтегрованими або SoftLogic [1].

Система збору даних та оперативного диспетчерського управління повинна виконувати наступні ключові функції: отримання інформації про контрольовані технологічні параметри від контролерів і датчиків нижніх рівнів; збереження зібраних даних в архівах; надання графічного відображення поточного процесу та архівної інформації у зручному форматі; прийом команд оператора і передача їх до контролерів та виконавчих механізмів; реєстрація подій, пов'язаних із процесом і діями персоналу; сповіщення про аварійні ситуації та реєстрація дій персоналу під час їхнього усунення; відображення архівних даних з можливістю порівняння в різних форматах і одночасно в кількох екземплярах [2].

SCADA (Supervisory Control and Data Acquisition) – це система для моніторингу та управління промисловими процесами та інфраструктурою в режимі реального часу. Вона забезпечує операторам можливість отримувати дані від різноманітних сенсорів і пристроїв, контролювати виконання процесів, оперативно виявляти несправності та автоматизувати певні дії на підприємствах та об'єктах критичної інфраструктури. SCADA широко застосовується у таких галузях:

– *енергетика*: управління електричними підстанціями, системами розподілу та передачі електроенергії;

– *водопостачання та водовідведення*: контроль насосних станцій, резервуарів, систем фільтрації та трубопроводів;

– *транспорт*: управління транспортними потоками на дорогах, залізничних системах, моніторинг роботи метро та аеропортів;

– *нафтогазова промисловість*: контроль процесів видобутку, переробки та транспортування нафти та газу;

– *виробництво*: автоматизація виробничих процесів на заводах і фабриках [3].

Система SCADA здатна збирати різноманітні дані з обладнання заводу, такі як показники температури, тиску та швидкості, за наявності підключення до цього обладнання. Зібрані дані є необробленими, і PLCs або RTUs перетворюють їх на інформацію, зрозумілу для операторів.

Важливою перевагою SCADA є її здатність збирати як поточні, так і історичні дані. Дані в режимі реального часу використовуються для моніторингу та обслуговування, тоді як історичні дані допомагають у створенні звітів і підвищенні ефективності виробництва.

Для SCADA не є обов'язковою умова використання обладнання одного постачальника, щоб перетворювати дані на зрозумілу інформацію. Головне – наявність сумісного протоколу зв'язку, який підтримують PLCs або RTUs. Це забезпечує ефективний обмін інформацією між різними виробничими об'єктами.

У галузі вітрової енергетики міжнародний стандарт IEC 61400-25 використовується для зв'язку, що дає змогу моніторити та керувати вітровими електростанціями, забезпечуючи обмін даними незалежно від виробника станцій [3].

Основні аспекти захисту SCADA включають:

– *сегментація мережі*: поділ мережі на окремі сегменти з метою обмеження доступу та зменшення ймовірності поширення атак;

– *аутентифікація та контроль доступу*: використання багаторівневої аутентифікації та строгих політик доступу для захисту від несанкціонованих дій;

– *шифрування даних*: забезпечення конфіденційності інформації під час її передачі;

– *моніторинг та виявлення загроз*: використання систем виявлення вторгнень (IDS) та систем управління інформаційною безпекою (SIEM) для своєчасного виявлення аномалій;

– *регулярне оновлення ПЗ*: своєчасне оновлення програмного забезпечення та встановлення патчів для усунення відомих вразливостей;

– *навчання персоналу*: підвищення обізнаності працівників про основи кібербезпеки для зменшення людського фактору ризику.

Висновки. Захист систем управління промисловими процесами (SCADA) підкреслює важливість комплексного підходу для забезпечення їхньої безпеки. Оскільки SCADA-системи контролюють критично важливі інфраструктури, такі як енергетика, водопостачання, транспорт та виробництво, їх захист має пріоритетне значення. Сучасні кіберзагрози стають дедалі складнішими та різноманітнішими, що підвищує ризик атак і потенційних збоїв у роботі цих систем.

Інформаційні джерела

1. SCADA. URL: https://uk.wikipedia.org/wiki/SCADA (дата звернення 16.11.2024).

2. Призначення, структура і основні функції SCADA-систем. URL: http://www.votum.ua/old/uk/publications/scada.htm (дата звернення 16.11.2024).

3. What is SCADA? URL: https://scada-international.com/what-is-scada/?utm_medium=cpc&utm_source=google.com&utm_campaign=scada-explained&gad_source=1&gclid=Cj0KCQiAouG5BhDBARIsAOc08RTFbfBJMuwzgVavSC9SmxoYhSnQtZp3vZ45z7xeAZPIvpofta2T8QoaArjjEALw_wcB#whatisscada (дата звернення 16.11.2024).

УДК 654.01

ДОСЛІДЖЕННЯ СПОСОБІВ ЗАХИСТУ WEB-САЙТІВ ВІД МЕРЕЖЕВИХ АТАК

Орест ПОЛОТАЙ

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The main methods of comprehensive protection of WEB-sites from network attacks are described. The rules of safe behavior when working with WEB-sites are considered.*

Keywords: *information security, WEB site protection.*

Анотація. *Описано основні способи комплексного захисту WEB-сайтів від мережевих атак. Розглянуто правила безпечного поводження поводження при роботі з WEB-сайтами.*

Ключові слова: *інформаційна безпека, захист WEB-сайтів.*

Безпека є дуже важливою складовою будь-якої програми. Основною причиною більшості взломів в веб-додатках є написаний розробниками програмний код. Саме тому захист WEB-сайтів починається на етапі їх розроблення. Також для безпечного користування потрібно дотримуватися всіх правил безпеки WEB-сайтів.

1. Дотримання всіх правил

Існує багато законів та правил для створення WEB-сторінки та її захисту. Одне з яких є створення КСЗІ (комплексна система захисту інформації), цей комплекс є сукупністю організаційних та технічних заходів для забезпечення захисту інформації.

2. Блокування користувачів

Передбачити блокування користувачів, що порушують правила КСЗІ та забезпечити блокування доступу до WEB-сторінки.

3. Захист приміщення

Захист приміщення, де знаходяться сервери та обчислювальна система WEB-сайту. Доступ до цього приміщення має здійснюватись тільки, якщо це передбачає договір міє власником WEB-сторінки та оператором (провайдером). Захистити приміщення від зловмисників можна шляхом встановлення охоронної системи.

Охоронна система – автоматизований комплекс для охорони різних об’єктів майна (будівель, включаючи прилеглу до них територію, окремих приміщень, автомобілів, водного транспорту, сейфів та ін.) Термін є узагальнюючим для декількох типів систем.

Основне призначення – попередити, по можливості запобігти або сприяти запобіганню ситуацій, в яких буде завдано шкоду людям або матеріальним

і не матеріальним цінностям, пов'язаних насамперед з діями інших осіб. Дієвим способом програмно-технічного захисту інформації, є крипто-захист, тобто системи, що дозволяють шифрувати та дешифрувати інформаційні потоки. Традиційна криптографія виходила з того, що для шифрування та дешифрування використовується один і той же секретний ключ, який мав мати відправник повідомлення і отримувач. Одним з поширених, сьогодні, методів шифрування є алгоритм RSA, в основі якого кожен учасник процесу має власний таємний ключ та відкритий ключ, що не є секретним з допомогою якого проводиться обмін повідомленнями. Електронний цифровий підпис (ЕЦП) – це аналог власного підпису посадової особи в електронному вигляді.

4. Ідентифікація і автентифікація

Комплекс засобів заходу повинні ідентифікувати категорію користувача WEB-сторінки та за атрибутами категорії надати доступи та послуги, які належать до цієї категорії. Ідентифікація здійснюється за допомогою імені та/або IP-адреси користувача.

5. Збирання та обробка персональних даних

Внесенням персональних даних на сайт, користувач підтверджує обробку цих даних. Тому, обробкою та збереження цих даних має займатися довірена людина. Також WEB-сайт, повинен забезпечити заходи, які відповідають за перевірку цілісності цих даних та їх захисту

6. Системи заходу

З своєї сторони користувач може використовувати програмно-апаратні засоби для виявлення та усунення несанкціонованого доступу та аналізу шкідливого програмного забезпечення. Прикладом таких систем є IPS\IDS системи. Також користувач може використовувати брандмауер для фільтрації шкідливого та небезпечного з'єднання та контенту.

Можна виділити кілька основних способів захистити WEB-сайт від мережевих атак:

1. Забезпечити захист від DDoS-атак – Якщо ваш хостинг-провайдер надає послуги захисту від DDoS-атак або ви користуєтеся послугами анти-DDoS-сервісів, то це питання можна вважати закритим, але чому б не посилити захист і не організувати її своїми руками, що безсумнівно є трудомістким завданням і передбачає одночасне використання таких технік: якщо в якості веб-сервера використовується Apache, то необхідно поставити перед ним проксі – Nginx або Lighttpd, а краще на фронтенді використовувати Nginx, але з декількома додатковими компонентами (обмежити розміри буферів та з'єднання Nginx, налаштувати тайм-аути і т. п.; використовувати модуль testcookie-nginx; використовувати фільтрацію по URL і віддавати нестандартний код 444, який дозволяє закрити з'єднання і не віддавати нічого у відповідь); у деяких випадках використовувати блокування за географічною ознакою; автоматизувати процес аналізу логів веб-сайту, звертаючи особливу увагу на обсяг трафіку, час відповіді сервера, кількість помилок і кількість запитів в секунду.

2. Підключити SSL-сертифікат – завдяки HTTPS-з'єднанню, яке забезпечує SSL-сертифікат, усі дані, які передаються через сервер, шифруються і не можуть бути перехоплені хакерами. SSL-сертифікат наразі є стандартом безпеки, особливо для e-commerce-сайтів, на яких відбуваються транзакції. До того ж сам Google настійливо рекомендує сайтам використовувати шифрування HTTPS і вище ранжує такі ресурси у пошуковій видачі.

3. Використовувати надійний хостинг – якісний хостинг-провайдер завжди надасть належний рівень безпеки сайтам своїх клієнтів. Як мінімум це резервне копіювання, завдяки якому можна відновити усі дані сайту, якщо раптом щось піде не так. Як максимум – захист від DDoS та антивірус у тарифі.

4. Використовувати безпечні плагіни/бібліотеки/фреймворки/CMS (далі – "сторонні модулі");

5. Завжди оновлювати програмне забезпечення – регулярно оновлюйте антивірусне та інше супутнє програмне забезпечення вашого сайту. Якщо цього не робити, будь-яка людина, включаючи хакерів, може отримати несанкціонований доступ до конфіденційних даних через прогалини в безпеці, які могли б бути усунені під час оновлення до останньої версії програмного забезпечення. Крім того, необхідно переконатися, що ваші операційні системи оновлені та підтримуються виробником. Використання застарілої або непідтримуваної ОС зробить ваш сайт вразливим до шкідливих програм, витоку даних і, зрештою, втрати функціональності.

6. Робити регулярне резервне копіювання веб-сайту та всіх важливих даних – резервне копіювання даних має вирішальне значення для забезпечення безперервності вашого бізнесу. Бекапи дадуть вам змогу швидко відновитись після кібератаки або інших небажаних інцидентів, таких як поломка обладнання, приміром. Найпростіший спосіб забезпечити періодичне резервне копіювання – обрати хостинг-провайдера, який щоденно робить бекапи даних своїх клієнтів.

7. Використовувати надійні і складні паролі, а також захист від перебору паролів – Ідеальний пароль складається зі щонайменше 12 цифр, спеціальних символів і літер верхнього та нижнього регістрів, не містить особисту інформацію, *наприклад* ім'я/день народження, яку можна дізнатися з мережі, кожен акаунт має свій пароль. Періодично змінюйте паролі. Для фінансових онлайн-рахунків це потрібно робити двічі на місяць. Паролі для входу краще змінювати хоча б раз на квартал. Якщо використовувати один і той самий пароль протягом більш тривалого часу, ризик витоку даних в рази збільшується.

З кожним днем зростає ризик та ймовірність виникнення загроз інформаційної безпеки WEB-сайтів від мережевих атак. Постає необхідність в оцінці даних ризиків, з метою зменшення ймовірності їх появи а також зниження збитків від їх настання до мінімальних значень. Оцінка ризиків є важливою складовою будь-якого процесу інформаційної безпеки. Процедуру оцінювання ризиків використовують для визначення масштабів загроз безпеці інформації, ймовірності реалізації загрози, та наслідків, які вони спричиняють. При

оцінці ризиків необхідно приймати до уваги всі можливі джерела загроз WEB-сайтів, які можуть мати фатальний вплив або непереборні наслідки.

Висновки. Кожна окрема рекомендація заслуговує окремого розгляду, але навіть при такому короткому розгляді залишається зрозумілим наступне – підхід до забезпечення безпеки повинен бути комплексним і системним. Необхідно ретельно підходити до контролю доступу, підтримувати в актуальному стані наявні сторонні модулі, фільтрувати вхідні дані та багато іншого.

Інформаційні джерела

1. Belej O., Nestor N., Sadeckii J., Polotai O. I. Features of Application of Data Transmission Protocols in Wireless Networks of Sensors. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019. Proceedings. 2019. Article ID 8847878, pp. 317–322.

2. Веб сайт компанії Altersign. URL: http://altersign.com.ua/korysna-informacija/pobudova-kszi/shcho-take-kompleksna-systema-zahystu-informaciji-kszi.

3. Полотай О. І., Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи. Зб. тез. ІІІ Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах" (м. Львів, 28 листопада 2019 р.). Львів : ЛДУБЖД, 2019. – С. 76–78.

4. Полотай О. І., Ігнатюк Л. О. Проектування комплексної системи захисту інформації львівської філії ПрАТ "Київстар". Зб. тез доп. І Міжнар. наук.-техн. конф. "Інформаційна безпека в сучасному суспільстві" (м. Львів, 21–22 листопада 2014 р.). Львів : ЛДУБЖД, 2014.

5. Полотай О. І., Деменко В. Особливості оцінки ризиків загроз інформаційної безпеки. Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів "Проблеми та перспективи забезпечення безпеки життєдіяльності" (м. Львів, 24 березня 2016 р.). Львів : ЛДУБЖД, 2016. – С. 204–205.

УДК 343.9:159.9

ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРЗЛОЧИННОСТІ: МОТИВАЦІЯ ЗЛОВМИСНИКІВ

Нікіта ОДЕРІЙ
Віталій СВІТЛИЧНИЙ
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article examines the psychological and sociocultural aspects of cybercrime, which encompass the motives and character traits of perpetrators. The impact of economic inequality, low digital literacy, and weak legislation on the spread of cybercrime is analyzed. Particular attention is paid to the key motives of cybercriminals, including financial gain, the thirst for power, ideological beliefs, and the desire to prove*

technical mastery. A generalized profile of a cybercriminal is formed and the need to develop strategies to combat cybercrime is substantiated.

Keywords: *cybercrime, psychological aspects, sociocultural factors, financial gain, hacktivism, digital literacy, economic inequality, cybercriminal profile.*

Анотація. *Стаття досліджує психологічні та соціокультурні аспекти кіберзлочинності, які охоплюють мотиви та риси характеру зловмисників. Аналізується вплив економічної нерівності, низької цифрової обізнаності та слабкого законодавства на поширення кіберзлочинів. Особливу увагу приділено ключовим мотивам кіберзлочинців, серед яких фінансова вигода, жага влади, ідеологічні переконання та прагнення довести технічну майстерність. Формується узагальнений профіль кіберзлочинця та обґрунтовується необхідність розробки стратегій боротьби з кіберзлочинністю.*

Ключові слова: *кіберзлочинність, психологічні аспекти, соціокультурні фактори, фінансова вигода, хактивізм, цифрова обізнаність, економічна нерівність, профіль кіберзлочинця.*

Кіберзлочинність у сучасному світі стає все більш багатогранною проблемою, що охоплює як індивідуальні, так і організовані злочинні дії, спрямовані на отримання фінансової вигоди, досягнення влади, ідеологічного впливу або навіть задоволення психологічних потреб, таких як пошук адреналіну чи демонстрація технічної майстерності. В основі таких дій часто лежать спільні риси, як-от високий інтелект, схильність до ризику та низький рівень емпатії, що дозволяє злочинцям ігнорувати морально-етичні наслідки своїх дій. Водночас значний вплив мають і економічна нерівність і низька цифрова обізнаність населення та слабке законодавство у сфері кібербезпеки створюють сприятливі умови для поширення кіберзлочинів. Аналіз цих психологічних і соціокультурних аспектів не лише дозволить краще зрозуміти природу кіберзлочинності, а й буде слугувати основою для розробки ефективних стратегій її протидії.

Одним із ключових мотивів скоєння кіберзлочинів є фінансова вигода. Зловмисники шукають способи швидкого збагачення, використовуючи викрадення даних, фінансове шахрайство або вимагання викупу за допомогою програм-шифрувальників. Інші кіберзлочинці можуть бути мотивовані жадобою влади, прагнучи контролювати системи або отримувати доступ до конфіденційної інформації. Крім того, ідеологічні переконання, як у випадку активістів, можуть штовхати людей до атак, які мають на меті політичні або соціальні зміни. Шукаючи адреналін, деякі молоді хакери прагнуть довести власні технічні здібності. Серед кіберзлочинців часто зустрічаються особи з високим рівнем інтелекту, оскільки здійснення складних атак потребує технічної майстерності та аналітичного мислення. Вони нерідко виявляють схильність до ризику, готовність іти на небезпеку, особливо в разі, коли їхні

дії можуть бути помічені правоохоронними органами. Інша характерна риса – низький рівень емпатії, адже багато кіберзлочинців сприймають своїх жертв як безликі об'єкти, ігноруючи етичні наслідки своїх дій. Соціальні та культурні умови також відіграють значну роль у мотивації кіберзлочинців. *Наприклад*, в економічно нестабільних країнах люди, які мають високі технічні здібності, можуть звертатися до кіберзлочинності через брак легальних можливостей для працевлаштування. Крім того, суспільства з низьким рівнем цифрової обізнаності створюють сприятливе середовище для фішингових та інших соціоінженерних атак.

Мотиви кіберзлочинців часто мають схожість із рисами їхнього характеру. *Наприклад*, жага влади або адреналіну може поєднуватися з ризиковою поведінкою, а прагнення фінансової вигоди – з аналітичним мисленням. Проте різниця полягає в тому, що одні злочинці діють із раціональних причин, *наприклад*, через економічний тиск, а інші керуються особистими прагненнями або ідеологічними установками. Соціокультурний контекст може різнитися залежно від типу кіберзлочинців. Для хактивістів соціальна несправедливість або політична нестабільність можуть бути рушійними силами, натомість для фінансово мотивованих злочинців економічна нерівність або слабке законодавство у сфері кібербезпеки відкривають додаткові можливості для здійснення атак. Розуміння психологічних мотивів кіберзлочинців ускладнюється через їхню анонімність, а наявність різних груп, від аматорів до організованих злочинних організацій, потребує різних підходів до аналізу. Також соціокультурний вплив може бути не завжди очевидним, оскільки злочинці часто діють глобально, використовуючи транскордонний характер Інтернету.

Висновки. Психологічні та соціокультурні аспекти дозволяють сформувати узагальнений профіль кіберзлочинця, що включає поєднання інтелектуальних здібностей, прагнення уникнути покарання, низьку емпатію та мотивацію, яка корелює із соціальними умовами. Вивчення цих аспектів допомагає розробляти більш ефективні стратегії боротьби з кіберзлочинністю, включаючи створення соціальних програм, спрямованих на зменшення економічного тиску, та просвітницькі кампанії для підвищення цифрової грамотності.

Інформаційні джерела

1. Проблема кіберзлочинності. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4-2.pdf (дата звернення: 19.11.2024).

2. Кіберзлочинність у всіх її проявів. URL: https://www.gurt.org.ua/articles/34602/ (дата звернення: 19.11.2024).

3. Кіберзлочинність: Правові аспекти та методи боротьби. URL: https://consultant.net.ua/consultant-article/6003 (дата звернення: 19.11.2024).

4. Кіберзлочинність: актуальна судова практика. URL: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika (дата звернення: 19.11.2024).

УДК 004.056.5:340

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВУ ЕПОХУ: НОРМАТИВНО-ПРАВОВИЙ АСПЕКТ

Артур ФЕДОРЕНКО

Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *Analysis of key tools for ensuring the protection of personal data in the modern digital environment: AES-256 encryption, the OneTrust privacy management system and Norton antivirus software. The functionality, advantages and limitations of each tool are considered, as well as their role in a comprehensive cybersecurity strategy. Particular attention is paid to the effectiveness, accessibility and areas of application of these solutions.*

Keywords: *AES-256, OneTrust, Norton AntiVirus, personal data protection, confidentiality, encryption, antivirus software, cybersecurity.*

Анотація*. Аналіз ключових інструментів для забезпечення захисту персональних даних у сучасному цифровому середовищі: шифрування AES-256, систему управління конфіденційністю OneTrust та антивірусне програмне забезпечення Norton. Розглянуто функціональні можливості, переваги та обмеження кожного інструмента, а також їхню роль у комплексній стратегії кібербезпеки. Особлива увага приділяється ефективності, доступності та сферам застосування цих рішень.*

Ключові слова: *AES-256, OneTrust, Norton AntiVirus, захист персональних даних, конфіденційність, шифрування, антивірусне програмне забезпечення, кібербезпека.*

У сучасному цифровому середовищі, яке характеризується широким використанням персональних даних, питання захисту інформації набуває ключового значення. Зростання обсягів збережених і оброблюваних даних, а також еволюція кіберзагроз підвищують важливість інструментів і сервісів, які забезпечують конфіденційність, цілісність та доступність даних. Це дослідження аналізує найпоширеніші сервіси для забезпечення захисту персональних даних, функціональні можливості яких та внесок у створення безпечного цифрового середовища.

Порівняльний аналіз шифрування даних AES-256, системи управління конфіденційністю One Trust та антивірусного програмного забезпечення Norton. Розпочнемо з AES-256, що використовується для шифрування даних з метою їхньої конфіденційності та захисту під час передачі або зберігання. OneTrust фокусується на управлінні конфіденційністю, допомагаючи організаціям відповідати міжнародним регуляторним вимогам, як-от GDPR або CCPA. Таке комплексне рішення для моніторингу та автоматизації обробки даних розроблено для захисту від шкідливого програмного забезпечення, включаючи віруси, трояни та шпигунські програми. Воно орієнтоване пере-

важно на кінцевих користувачів і забезпечує їхній пристроям активний захист. AES-256 є симетричним алгоритмом шифрування, який використовує 256-бітний ключ для перетворення даних на шифротекст. Його головна перевага – висока стійкість до злому, що забезпечує безпеку навіть перед складними атаками. В свою чергу OneTrust базується на автоматизації процесів управління конфіденційністю, забезпечуючи прозорість обробки даних і дотримання законодавства, що дозволяє відстежувати транзакції зі згодою користувачів та управляти ними. А Norton AntiVirus використовує підхід до виявлення шкідливих програм у реальному часі, застосовуючи оновленні бази даних та інструменти для ізоляції шкідливих програм.

AES-256 використовується широким колом користувачів – від окремих осіб до корпоративних клієнтів та урядових установ, які працюють з чутливою інформацією. OneTrust орієнтований переважно на великі організації та корпорації, які зобов'язані дотримуватися суворих нормативних вимог у сфері конфіденційності. Norton AntiVirus здебільшого розрахований на індивідуальних користувачів і малий бізнес, які потребують захисту своїх пристроїв і особистих даних.

OneTrust дозволяє централізовано керувати конфіденційністю, відповідністю вимогам і взаємодією з клієнтами, забезпечуючи високий рівень довіри до бренду. AES-256 забезпечує високий рівень безпеки та є стійким до більшості сучасних атак. Його універсальність дозволяє використовувати його у різних сценаріях. Norton AntiVirus є простим у використанні рішенням із регулярними оновленнями, що підтримує актуальність захисту від нових загроз.

AES-256 залежить від правильного зберігання ключів шифрування. Втрата ключа робить розшифрування даних неможливим. OneTrust є досить складним у впровадженні та може вимагати значних ресурсів для інтеграції в існуючі процеси. Norton AntiVirus іноді критикують за пропуски у виявленні специфічних загроз, зокрема шпигунських програм, та за зниження продуктивності пристроїв.

OneTrust є високовартісним корпоративним рішенням, але його функціонал виправдовує інвестиції для великих організацій. AES-256 інтегрований у багато безкоштовних і комерційних програмних рішень, що робить його доступним для широкої аудиторії. Norton AntiVirus пропонує як безкоштовні, так і платні версії, що робить його доступним для більшості користувачів, хоча деякі функції доступні лише за підпискою.

Norton AntiVirus залежить від актуальності оновлень баз даних, і його ефективність зменшується, якщо користувач не підтримує програму у належному стані. AES-256 може бути вразливим до квантових обчислень у майбутньому, що створює потребу в нових криптографічних алгоритмах. OneTrust стикається зі складнощами інтеграції та адаптації до часто змінюваних нормативних вимог.

Висновки. Кожен з розглянутих інструментів відіграє важливу роль у забезпеченні кібербезпеки, маючи свої унікальні переваги. AES-256 забезпечує базову безпеку даних, OneTrust зосереджується на відповідності та управлінні конфіденційністю, а Norton AntiVirus активно захищає кінцеві пристрої від шкідливих програм. У поєднанні ці рішення створюють потужний комплексний підхід до захисту персональних даних.

Інформаційні джерела

1. AES-256. URL: https://www.vpnunlimited.com/ua/help/cybersecurity/aes-256 (дата звернення: 15.11.2024).

2. OneTrust назвала абсолютного лідера в звіті про управління конфіденційністю і згодою. URL: https://itpro.kiev.ua/post/onetrust_nazvan_absolyutnym_liderom_v_otchete_ob_upravlenii_konfidentsialnostyu_i_soglasiem/ (дата звернення: 19.11.2024).

3. Norton AntiVirus. URL: https://uk.wikipedia.org/wiki/Norton_AntiVirus (дата звернення: 18.11.2024).

УДК 654.01

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ БЕЗПЕЧНИХ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ VLAN

Орест ПОЛОТАЙ
Максим ГУМЕНЮК

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The main methods of implementing virtual local area networks are described, for dividing a local area network into separate groups of smaller networks within small broadcast domains.*

Keywords: *information security, virtual local area networks.*

Анотація. *Описано основні способи реалізації віртуальних локальних мереж, для поділу локальної мережі на окремі групи менших мереж в межах дрібних широкомовних доменів.*

Ключові слова: *інформаційна безпека, віртуальні локальні мережі*.

Віртуальна локальна мережа (VLAN) – це логічна мережа, яка створюється в межах більшої фізичної мережі. Основним призначенням технології VLAN є полегшення процесу ізолювання мереж, які згодом будуть пов’язані маршрутизаторами, що реалізують один із протоколів мережевого рівня, *наприклад*, IP. Даний вид організації мережі дозволяє забезпечувати досить потужні бар’єри на шляху помилкового трафіку при

його передачі з однієї мережі в іншу, таким чином забезпечуючи захист інформаційних потоків в межах окремих доменів.

Мережі VLAN реалізовуються на базі комутаторів, їх можна створювати як на базі одного комутатора так і декількох.

Комутатор або світч – це пристрій мережі, призначений для забезпечення з'єднання між пристроями в локальній мережі (LAN). Він дозволяє ефективно управляти мережевим трафіком, відправляючи дані тільки туди, де вони дійсно необхідні. На відміну від маршрутизаторів, підключення здійснюється тільки по кабелю. Іншими словами, пристрій не забезпечує розгортання бездротової мережі. На відміну від концентраторів, які поширює трафік від одного підключеного пристрою до всіх інших пристроїв, комутатор надсилає дані лише безпосередньому одержувачеві. Це усуває необхідність (і можливості) обробки даних іншими сегментами мережі, які їм не призначені, що підвищує продуктивність і безпеку мережі.

Для створення віртуальних мереж на основі одного комутатора (рис. 1) найчастіше застосовується спосіб групування мережі портів комутатора, при якому кожен порт зараховується певної віртуальної мережі. Широкомовний кадр, що надійшов від порту, який відноситься, *наприклад*, до VLAN 1, ніколи не буде надіслано порту, який не знаходиться у цій VLAN. Порт також можна віднести до кількох VLAN, але практично цей спосіб використовується рідко, оскільки зникає ефект повної ізоляції мереж.

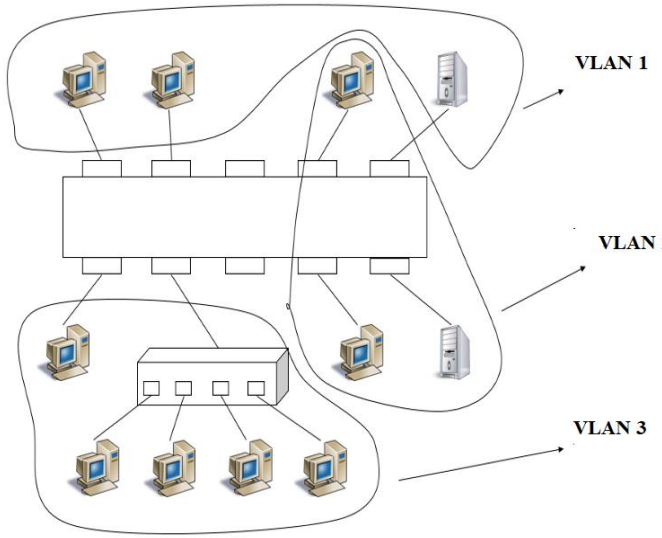


Рисунок 1 – Побудова VLAN на базі одного комутатора способом групування портів

Найбільш логічним і поширеним способом створення VLAN є групування портів одного комутатора, оскільки віртуальних мереж, побудованих з урахуванням одного комутатора, може бути більше, ніж портів. У випадках, коли до одного порту приєднаний сегмент, створений на основі повторювача, недоцільно підключати вузли даного сегмента до різних віртуальних мереж, так як у будь-якому випадку трафік цих вузлів залишиться загальним. Для утворення віртуальних мереж на основі групування портів достатньо зарахувати кожен порт до однієї з кількох вже названих віртуальних мереж, тобто від користувача не потрібно великого обсягу ручної роботи. Найчастіше цей процес проводиться з використанням спеціальної програми, яка додається до комутатора. Адміністратор створює віртуальні мережі за допомогою переміщення мишею графічних символів портів на графічні символи мереж.

При використанні мережі VLAN у мережах з деякою кількістю зв'язаних між собою комутаторів, на каналах зв'язку, що знаходяться між ними, використовується магістральне з'єднання VLAN (VLAN trunking). Магістральне з'єднання VLAN передбачає застосування комутаторами процесу призначення тегів VLAN (англ. VLAN tagging), при якому перед початком передачі кадру через магістральний канал комутатор доповнює цей кадр іншим заголовком. Даний додатковий заголовок складається з поля ідентифікатора VLAN (англ. VLAN ID), який дає можливість комутатору, що передає, зіставляти кадр з певною мережею VLAN, а приймає комутатору визначити, до якої конкретно VLAN відноситься цей кадр.

На рисунку 2 можна побачити приклад двох мереж VLAN з кількома комутаторами, однак без використання магістрального з'єднання. У цьому випадку застосовуються дві мережі VLAN: VLAN 1 і VLAN 2. Кожній з мереж VLAN належить по два порти на кожному комутаторі, отже,

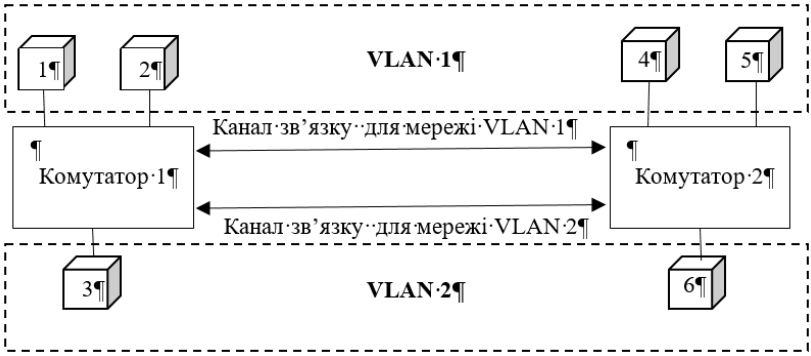


Рисунок 2 – Мережі VLAN на базі декількох комутаторів без магістрального з'єднання

кожна мережа VLAN присутня в обох комутаторах. Для перенаправлення інформаційного потоку мережі VLAN 1 між двома комутаторами, до яких вона належить, дана схема передбачає присутність каналу зв'язку між ними, який в повному обсязі розташовується в мережі VLAN 1. Так само, для забезпечення трафіку мережі VLAN 2 між комутаторами знаходиться другий канал зв'язку, що вже повністю знаходиться в мережі VLAN 2.

Комп'ютер 1 (що знаходиться в мережі VLAN 1) повною мірою може передати кадр комп'ютеру 5. Фрейм попрямує на комутатор 1, після чого через канал зв'язку (призначений для VLAN 1) попрямує на комутатор 2. Однак, незважаючи на те, що ця схема працює, її масштабування є нелегким завданням. Для кожної мережі VLAN потрібен окремий фізичний канал зв'язку між комутаторами. *Наприклад*, при необхідності наявності 10 або 20 мереж VLAN, необхідно розташувати між 10 або 20 комутаторами каналів зв'язку і застосувати для них 10 або 20 портів на кожному комутаторі.

Магістральне з'єднання VLAN утворює між комутаторами один канал зв'язку, який може підтримувати таку кількість мереж VLAN, яку потрібно. Для комутаторів цей магістральний канал буде частиною всіх VLAN. Але незважаючи на це, трафік у магістральному каналі VLAN буде роздільним, і кадри VLAN 1 ніяк не зможуть потрапити на пристрої VLAN 2 (і навпаки), оскільки, проходячи через магістральний канал, кожен кадр позначений номером VLAN. На рисунку 3 можна побачити схему мережі з фізичним каналом зв'язку між двома комутаторами.

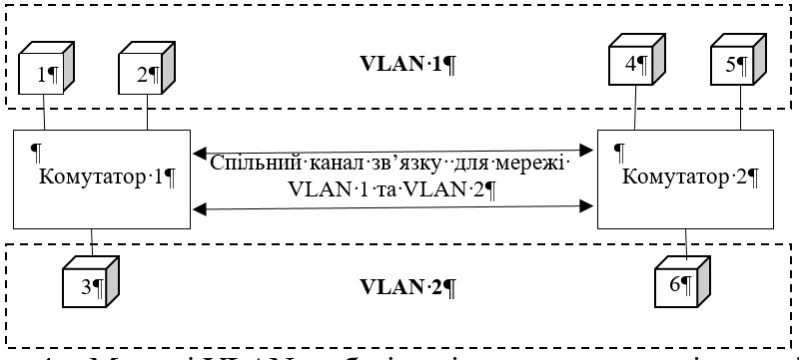


Рисунок 3 – Мережі VLAN на базі декількох комутаторів
з магістральним з'єднання

За допомогою магістрального з'єднання існує можливість пересилати інформаційні потоколи різних мереж VLAN по одному єдиному фізичному середовищу. При цьому не порушуючи правильна розмежування інформаційних потоків між різними мережами VLAN.

Висновки. Застосування технології віртуальних мереж у комутаторах дозволяє вирішити два завдання:

1. Підвищення продуктивності кожної з віртуальних мереж, оскільки комутатор передає кадри у подібній мережі лише вузлу призначення;

2. Ізоляція мереж один від одного для управління правами доступу користувачів та створення захисних бар'єрів на шляху широкомовних штормів.

Інформаційні джерела

1. Belej O., Nestor N., Sadeckii J., Polotai O. I. Features of Application of Data Transmission Protocols in Wireless Networks of Sensors. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019. Proceedings. 2019. Article ID 8847878, pp. 317–322.

2. Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. Вінницький національний технічний університет. КОМП'ЮТЕРНІ МЕРЕЖІ. Вінниця ВНТУ 2020.

3. Дубик А.-О. Ю., Полотай О. І. Загрози інформації в комп'ютерних мережах на канальному рівні. "Світ наукових досліджень" (матеріали Міжнародної мультидисциплінарної наукової інтернет-конференції (м. Тернопіль, Україна, м. Ополе, Польща, 21–21 березня 2024 р.). Вип. 28. – С. 185–187.

4. Дубик А.-О. Ю., Полотай О. І. Особливості захисту інформації в комп'ютерних мережах. "Світ наукових досліджень" (матеріали Міжнародної мультидисциплінарної наукової інтернет-конференції (м. Тернопіль, Україна, м. Ополе, Польща, 24–25 жовтня 2023 р.). Вип. 23. – С. 291–292.

5. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). URL: https://ela.kpi.ua/server/api/core/bitstreams/e5c73b24-058a-42d8-bd2d-03a17e2c7c9a/content

УДК 004.8:004.056

ШТУЧНИЙ ІНТЕЛЕКТ В ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Костянтин ПІЛЬОВ

Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The paper examines the current challenges of cybercrime, focusing on its key types, such as phishing, hacking, malware, and disinformation. Particular attention is paid to the use of artificial intelligence (AI) to combat cybercrime and its application in other areas, in particular for automatic vulnerability scanning, traffic violation detection, and chatbot operation. Both the potential of AI in security and its limitations are analyzed, emphasizing the need for further research and development of technologies.*

Keywords: *cybercrime, phishing, malware, disinformation, artificial intelligence, DDOS attacks, chatbots, digital security, automation.*

Анотація. *Робота розглядає сучасні виклики кіберзлочинності, акцентуючи увагу на її ключових видах, таких як фішинг, злом, шкідливе програмне забезпечення та дезінформація. Особлива увага приділяється використанню штучного інтелекту (ШІ) для протидії кіберзлочинам і його застосуванню в інших сферах, зокрема для автоматичного пошуку вразливостей, фіксації порушень правил дорожнього руху та функціонування чат-ботів. Аналізується як потенціал ШІ у сфері безпеки, так і його обмеження, підкреслюючи необхідність подальших досліджень і розвитку технологій.*

Ключові слова: *кіберзлочинність, фішинг, шкідливе програмне забезпечення, дезінформація, штучний інтелект, DDOS-атаки, чат-боти, цифрова безпека, автоматизація.*

У сучасному світі дуже гостро стає питання що до боротьби з кіберзлочинністю. Що таке кіберзлочинність у сучасному розумінні. Кіберзлочинність – це злочинна діяльність, яка передбачає використання комп'ютерів, комп'ютерних мереж або мережевих пристроїв. Кіберзлочини здійснюють кіберзлочинці – люди, які використовують інформаційні технології у протиправний спосіб [4]. На разі, правопорушення у кіберпросторі поділяються на 3 види:

– *фішинг* – фейкові електронні листи, у яких просять зазначити конфіденційну інформацію або особисті дані. Здебільшого, вони містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн-відомих ресурсів;

– *злом* – коли злочинець насильно без дозволу намагається отримати доступ до вашого пристрою;

– *шкідливе програмне забезпечення* – програма, яка встановлюється на комп'ютер без вашого дозволу, і впливає або порушує роботу комп'ютера [2].

Під час широкомасштабного вторгнення російської федерації гостро постало питання про ще один кіберзлочин як поширення дезінформації. Більшість з них спрямовані на підрив довіри читачів до уряду або поширення неправдивих чуток про когось.

Прикладом цього може послугувати новина про те, Збройні Сили України вступили до ЦАХАЛУ [1] або фейк про те, що у сумській області формується перша в Україні бригада дітей, для виконання бойових завдань [3]. Зрозуміло, що це все є дезінформацією. Що до шкідливих програмних забезпечення (ШПЗ), то їх теж використовують для проведення кібервійни. Їм можно протидіяти використовуючи штучний інтелект. Є можливість використовувати для автоматичного пошуку вразливостей у системі, що допоможе у покращенні системи безпеки державних електронних ресурсів та баз даних. Також, штучний інтелект, можна використовувати для атаки по ворожої онлайн сервісам та виводи, дистанційно, з ладу критичну інфраструктуру використовуючи DDOS-атаки. Але потрібно розуміти те, що потрібно використовувати його не тільки для боротьби з ворогом по за країною. Штучний інтелект також використовують у дорожніх камерах для фіксації по-

рушення правил дорожнього руху. Його алгоритм складеться з того, що він робить фото тільки тих машин, які порушують, встановлену на цій ділянці дороги, швидкість. Також в нього є алгоритм, який може визначити номер транспортного засобу, та його власника. Також штучним інтелектом являється чат-боти у соціальних мережах [5].

Чат-боти запрограмовані, щоб розпізнати завдання, що надходить, і надати кроки для його вирішення. Для цього програма виконує лінгвістичну обробку, щоб зрозуміти, що хоче користувач та яку інформацію потрібно йому продемонструвати. Прикладом такого чат-боту, який на цей час є для когось дуже важливим- це бот для пошуку зниклих по даних Національного інформаційного бюро з питань військовополонених та загиблих військовослужбовців внаслідок російсько-української війни [6]. Для тих, хто шукає родичів, які ймовірно, потрапили в полон чи загинули під час російсько-української війни.

Висновки. Для завершення своєї тези-доповіді, хочу сказати, що всі зазначенні у тексті приклади застосування штучного інтелекту мають свої переваги та недоліки. Щоб їх ставало все менше, потрібно досліджувати цю тему та розвивати її. Також, потрібно розуміти, що ШІ можна використовувати не тільки для протидії кіберзлочинів, а й використовувати для фіксації правопорушень у житті.

Інформаційні джерела

1. Дедей В. Россияне распространяют фейк о вступлении украинцев в ЦАХАЛ. Зеркало недели | Дзеркало тижня | Mirror Weekly. URL: https://zn.ua/UKRAINE/rossijane-rasprostranjajut-fejk-o-vstuplenii-ukraintsev-v-tsakhal.html (дата звернення: 04.11.2023).

2. Кіберзлочинність: як ідентифікувати та як діяти | Безпечне місто. Безпечне місто | Це справа кожного. URL: http://safe-city.com.ua/kiberzlochynnist-i-litni-lyudy/ (дата звернення: 04.11.2023).

3. Фейк: В Сумской области формируется первая в Украине “бригада детей”. StopFake. URL: https://www.stopfake.org/ru/fejk-v-sumskoj-oblasti-formiruetsya-pervaya-v-ukraine-brigada-detej/ (дата звернення: 04.11.2023).

4. Що таке кіберзлочинність?. NordVPN. URL: https://nordvpn.com/uk/cybercrimes/#:~:text=Кіберзлочинність%20–%20це%20злочинна%20діяльність,%20яка,інформаційні%20технології%20у%20протиправний%20спосіб. (дата звернення: 04.11.2023).

5. k-call.com. Що може штучний інтелект і де його застосовують – Keycall | Keycall. Голосовой бот, понимающий человеческую речь | Keycall. URL: https://k-call.com/ua/blog/iskusstvennyj-intellekt-v-obsluzhivanii-klientov-7-realnyh-primerov-ispolzovaniya (дата звернення: 04.11.2023).

6. Ukrinform. В Україні запустили чатбот для пошуку військовополонених та зниклих безвісти. Укрінформ – актуальні новини України та світу. URL: https://www.ukrinform.ua/rubric-society/3548893-v-ukraini-zapustili-catbot-dla-posuku-vijskovopolonenih-ta-zniklih-bezvisti.html (дата звернення: 04.11.2023).

УДК 004.838

ОСНОВНІ ПРОТОКОЛИ МЕРЕЖЕВОЇ БЕЗПЕКИ

Роман ЛИТВИНЕНКО
Василь ЛУЧИК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article examines the importance of network security in the context of the rapid development of information technology and threats associated with unauthorized access and cyberattacks. The main network protocols, their functions and role in ensuring confidentiality, integrity and authenticity of data are described. Particular attention is paid to the OSI model, which structures network protocols into seven layers, and to the main protocols, such as TCP/IP, SSL/TLS, DTLS, SNMP, Kerberos and DNS. The importance of implementing and regularly updating security protocols to adapt to modern cyber threats is emphasized.*
Keywords: *network security, security protocols, OSI model, TCP/IP, SSL/TLS, Kerberos, DNS, cyber threats, confidentiality, integrity, authenticity, network management.*

Анотація. *У статті розглядається значення мережевої безпеки в умовах стрімкого розвитку інформаційних технологій та загроз, пов'язаних із несанкціонованим доступом і кібератаками. Описуються основні мережеві протоколи, їхні функції та роль у забезпеченні конфіденційності, цілісності та автентичності даних. Особлива увага приділяється моделі OSI, яка структурує мережеві протоколи на сім рівнів, та основним протоколам, як-от TCP/IP, SSL/TLS, DTLS, SNMP, Kerberos і DNS. Наголошується на важливості впровадження та регулярного оновлення протоколів безпеки для адаптації до сучасних кіберзагроз.*
Ключові слова: *мережева безпека, протоколи безпеки, модель OSI, TCP/IP, SSL/TLS, Kerberos, DNS, кіберзагрози, конфіденційність, цілісність, автентичність, управління мережею.*

В умовах стрімкого розвитку інформаційних технологій та поширення використання мережі Інтернет питання мережевої безпеки стають дедалі актуальнішими. Захист даних під час їх передачі є критичним як для організацій, так і для звичайних користувачів, оскільки загрози, що пов'язані з несанкціонованим доступом та кібератаками, зростають щодня. Для забезпечення безпеки інформації використовуються різні протоколи, що відіграють важливу роль у захисті конфіденційності, цілісності та автентичності даних. Розуміння основних протоколів мережевої безпеки та їх застосування є ключовим для створення надійних систем, здатних протистояти сучасним загрозам та забезпечувати стабільну роботу мереж.

Мережевий протокол – це набір правил і стандартів, які визначають та регулюють процес обміну інформацією між комп'ютерами, підключеними

до інтернету. Протокол можна порівняти з мовою спілкування між машинами, що дозволяє їм взаємодіяти. Серед його головних характеристик – чітка структура та стандартизація [1].

Мережеві протоколи складаються з кількох рівнів, кожен з яких має свої завдання. Для моделювання цієї системи існує декілька фреймворків, але найпоширенішою є модель взаємозв'язку відкритих систем (OSI). Модель OSI поділяє стек мережевих протоколів на сім рівнів відповідно до їхніх функцій:

– фізичний рівень (рівень 1) – це фізичне підключення між системами, *наприклад*, електричні сигнали по кабелю;

– рівень каналу даних (рівень 2) – кодує трафік у біти, передає їх через фізичний рівень та забезпечує корекцію помилок;

– мережевий рівень (рівень 3) – здійснює маршрутизацію пакетів від джерела до місця призначення;

– транспортний рівень (рівень 4) – забезпечує повну доставку пакетів, контроль за розміром даних, послідовність і виправлення помилок;

– рівень сеансу (рівень 5) – відповідає за встановлення, управління та завершення з'єднань між програмами;

– презентаційний рівень (рівень 6) – виконує перетворення даних між мережевими пакетами і форматом, що використовується програмою;

– рівень додатків (рівень 7) – надає послуги та інструменти для програм високого рівня для комунікації через мережу [2].

Протоколи мережевої безпеки мають на меті забезпечити конфіденційність, цілісність і автентифікацію, або поєднання цих функцій для захисту мережевого трафіку. Серед основних прикладів таких протоколів:

Transmission Control Protocol / Internet Protocol (TCP/IP) – це набір протоколів, що визначають правила передачі даних у мережі. Основний принцип TCP/IP полягає в поділі інформації на окремі пакети, які передаються між пристроями. Кожен пакет містить дані про відправника і отримувача, що забезпечує надійну доставку, відновлення втрачених пакетів та контроль потоку даних. TCP/IP є основою мережевих систем CISCO для стабільного обміну інформацією між усіма пристроями в мережі [3].

SSL/TLS (рівень захищених сокетів та безпека транспортного рівня) – протокол безпеки, що працює у моделі OSI і надає шифрування, автентифікацію та захист цілісності даних у мережевому трафіку. З'єднання за допомогою SSL/TLS розпочинається з процедури рукостискання, яка встановлює безпечний зв'язок між клієнтом і сервером, під час якого обираються криптографічні алгоритми для шифрування, автентифікації та перевірки цілісності. SSL/TLS дозволяє обгортати інші протоколи у захищену, автентифіковану і перевірену оболонку [4].

DTLS – це протокол, призначений для забезпечення безпеки обміну датаграмами на основі TLS. Він не забезпечує гарантовану доставку повідом-

лень або їх отримання у правильному порядку. DTLS зберігає переваги використання дейтаграмних протоколів, зокрема меншу затримку та зниження накладних витрат [5].

Простий протокол керування мережею (SNMP) призначений для моніторингу та управління мережевими пристроями в організації. Менеджер SNMP може надсилати запити до пристроїв, а агент на цих пристроях надає відповіді або виконує необхідні дії. Ранні версії SNMP мали низький рівень безпеки, без функцій шифрування, автентифікації та забезпечення цілісності даних. SNMPv3, представлений у 2004 році, включає всі ці функції та використовує сучасні криптографічні алгоритми для захисту [2].

Kerberos – популярний протокол, що використовується для автентифікації запитів на обслуговування між довіреними системами через ненадійні публічні мережі. Основою протоколу є система квитків, які підтверджують особу користувача. Центральний сервер автентифікації перевіряє користувача і створює ці квитки, які потім можуть використовуватися для підтвердження права користувача робити певні запити. Kerberos підтримується більшістю операційних систем, таких як Windows, Mac і Linux, і є стандартним протоколом автентифікації для Windows, а також ключовим компонентом служби Active Directory (AD) [2].

DNS (domain name system) відповідає за перетворення читабельних адрес в IP-адреси, що запам'ятати значно складніше, і навпаки. Завдяки DNS ми можемо отримати доступ до інтернет-ресурсів за їх доменними іменами. Ця система є важливою під час роботи з доменами, *наприклад*, коли змінюється хостинг або реєстратор домену. Процес оновлення DNS-зони може тривати від 2 до 72 годин [6].

Висновки. У сучасному цифровому світі надійність та безпека передачі даних є одним із найважливіших аспектів функціонування мережевих систем. Основні протоколи мережевої безпеки, такі як SSL/TLS, IPSec, HTTPS, SSH та інші, забезпечують захист інформації під час її передачі, допомагаючи підтримувати конфіденційність, цілісність та автентичність даних. Їх впровадження дозволяє мінімізувати ризики несанкціонованого доступу, перехоплення та модифікації інформації. Однак для ефективного захисту необхідно регулярно оновлювати та вдосконалювати системи безпеки, адаптуючись до нових загроз та кібератак. Впровадження та правильне використання цих протоколів забезпечують надійний захист як для організацій, так і для користувачів, сприяючи стабільній і безпечній роботі мережевих систем.

Інформаційні джерела

1. Типи мережевих протоколів і їх призначення (HTTP, IP, SSH, FTP, POP3, MAC). URL: https://deltahost.ua/ua/tipi-merezhevix-protokoliv-i-ih-priznachennya-http-ip-ssh-ftp-pop3-mac.html?srsltid=AfmBOormpYtziGou1nuyeiSOPy7Rdu8OcqpueHLkEuhrtKDokM _uTcyb (дата звернення 16.11.2024).

2. Types of Network Security Protocols. URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/6-types-of-network-security-protocols/ (дата звернення 16.11.2024).

3. Огляд основних мережевих протоколів CISCO: як працюють TCP/IP, OSPF, BGP та інші. URL: https://optima.study/blog/ohlyad-osnovnykh-merezhevykh-protokoliv-cisco-yak-pratsyuyut-tcp-ip-ospf-bgp-ta-inshi#content1 (дата звернення 16.11.2024).

4. Network Security Protocols You Should Know. URL: https://www.catonetworks.com/network-security/network-security-protocols/ (дата звернення 16.11.2024).

5. Основні протоколи Мережі. Навіщо вони використовуються? URL: https://hyperhost.ua/info/uk/osnovni-protokoli-merezhi-navishcho-voni-vikoristovuyutsya (дата звернення 16.11.2024).

УДК 654.01

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ VPN

Іванна РОШИНЕЦЬ
Орест ПОЛОТАЙ
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The features of virtual private networks are described. The main components of such networks are shown, the structural diagram of VPN operation in an organization is shown. Statistics of VPN use in Ukraine and the world are given.*
Keywords: *information security, virtual private network.*

Анотація. *Описано особливості роботи віртуальних приватних мереж. Показано основні компоненти таких мереж, структурну схему роботи VPN в організація. Наводиться статистика використання VPN в Україні та світі.*
Ключові слова: *інформаційна безпека, віртуальна приватна мережа.*

У зв'язку з складними умовами сьогодення, які підготувала нам війна, а до того карантин, перед компаніями постало питання організації віддаленого режиму безпечної роботи для своїх співробітників, в разі критичної необхідності. Оскільки багато організацій раніше не реалізовували такий перехід, то швидке впровадження даного режиму роботи призвело до проблем з інформаційною безпекою. Одним із способів забезпечити безпеку даних при роботі в мережі, є використання технологій VPN.

VPN (скорочення від англ. virtual private network – віртуальна приватна мережа) – узагальнена назва клієнт-серверних технологій, які дають змогу створювати віртуальні захищені мережі поверх інших мереж із нижчим рівнем довіри.

VPN – це найлегший і найбільш ефективний спосіб захистити інтернет-трафік і забезпечити конфіденційність перебування в мережі. Після підключення до надійного VPN-сервера всі дані проходитимуть через зашифрований тунель, в якому їх ніхто не зможе побачити, ані хакери, ані урядові організації, ані інтернет-провайдер. На рис. 1 показана структура мереж VPN.

Рисунок 1 – Загальна структура мереж VPN

VPN забезпечує конфіденційність, цілісність та доступність інформації. Тобто гарантує те, що інформація не буде доступна небажаним особам, буде збережена та доступна лише визначеним користувачам. Дані характеристики забезпечується за допомогою основних компонентів VPN, які наведені на рисунку 2.

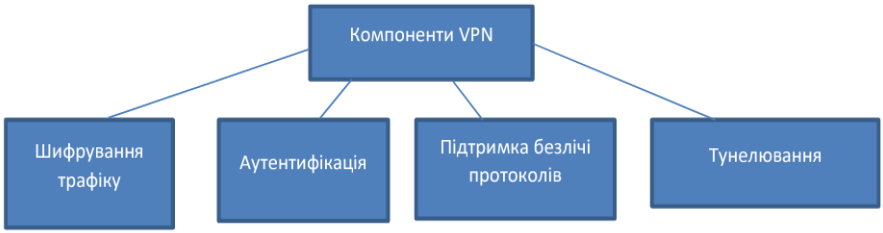


Рисунок 2 – Компоненти VPN

VPN – це спосіб розширення приватної мережі за допомогою загальнодоступної мережі, такої як Інтернет. Назва лише припускає, що це віртуальна “приватна мережа”. Це означає, що користувач може бути частиною локальної мережі у віддаленому місці. При цьому він використовує протокол тунелювання для встановлення безпечного з’єднання. І чим більший мережевий відділ компанії, тим більше у хакерів можливостей перехопити незахищену інформацію, тим вище захищеність каналів компанії.

На рисунку 3 представлена структурна схема мережі VPN організацій.

Будь-яка організація неминуче стикається з проблемою передачі інформації між офісами, а також з проблемою захисту цієї інформації. Не кожна організація може дозволити собі мати власний канал доступу. Цю проблему можна вирішити за допомогою технології VPN, заснованої на підключенні

всіх відділів та офісів. Це одночасно забезпечує гнучкість і високу безпеку мережі, що дозволяє значно економити кошти при створенні таких мереж.

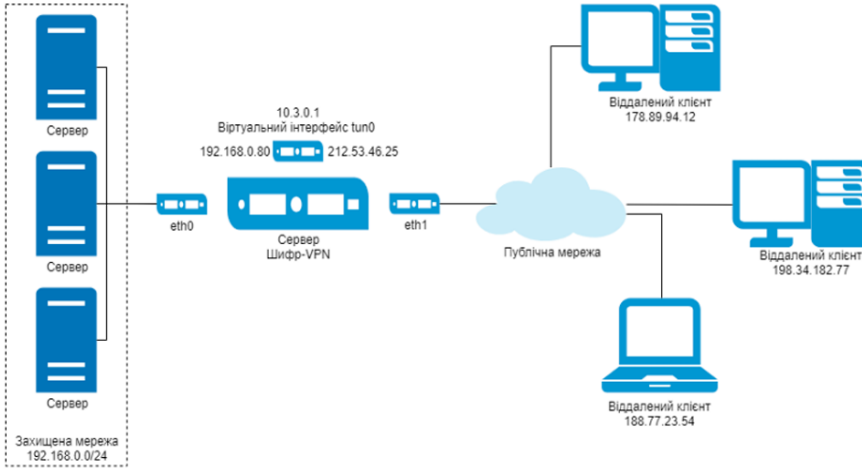


Рисунок 3 – Структурна схема мережі VPN організацій

VPN створюється на базі загальнодоступної мережі Інтернет. І якщо в Інтернет-комунікації і є недоліки, то головне, що вона схильна до потенційних порушень безпеки і конфіденційності. VPN може забезпечити захист трафіку, що передається через Інтернет, і його передачу в межах локальної мережі. У той же час віртуальні мережі забезпечують значну економію коштів у порівнянні з обслуговуванням вашої власної глобальної мережі.

Особливістю роботи VPN є пересилка даних через безпечний (зашифрований) тунель, організований в межах загальнодоступної мережі. Тунелювання дозволяє організувати передачу пакетів одного протоколу в логічному середовищі, використовуючи інший протокол. В результаті виникає можливість вирішити проблеми взаємодії декількох різнотипних мереж, починаючи з необхідності забезпечення цілісності і конфіденційності передаваних даних і закінчуючи подоланням невідповідностей зовнішніх протоколів або схем адресації.

Найбільш поширений метод створення тунелів VPN – інкапсуляція мережевого протоколу IP в PPP і подальша інкапсуляція утворених пакетів в протокол тунелювання. Такий підхід називають тунелюванням другого рівня, оскільки тут являється протокол на другому рівні.

На рисунку 4 продемонстровано схему захищеного каналу VPN.

Особливість технології VPN в тому, що організація віддаленого доступу робиться через Інтернет, що набагато дешевше і краще. Для організації

віддаленого доступу до приватної мережі за допомогою технології VPN знадобиться Інтернет і реальна IP-адреса а також програмне забезпечення.

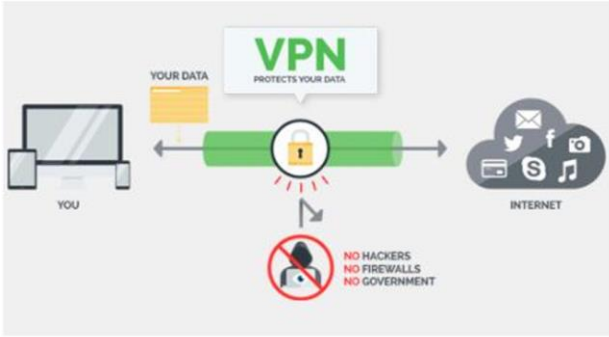


Рисунок 4 – Структурна схема мережі VPN організацій

Згідно з Глобальним індексом впровадження VPN від Atlas VPN, минулого року загальна кількість завантажень програмного забезпечення для організації VPN у світі склала 328 млн, це на 25 млн менше ніж у 2022 (353 млн). У 2021 році ця цифра була у 785 млн.

Pos.	Country	Downloads				Population	VPN adoption index		
		2023	2022	2021	2020		2023	2022	2021
1	Qatar	2 012 318	1 129 081	2 007 756	1 528 763	2.88M	69.87%	39.2%	69.69%
2	United Arab Emirates	6 101 770	4 270 047	5 886 566	6 093 301	9.89M	61.7%	43.18%	59.52%
3	Singapore	3 142 042	2 170 865	2 874 601	945 425	5.85M	53.71%	37.11%	49.14%
4	Oman	1 986 271	1 356 303	1 718 353	1 805 478	5.11M	38.87%	26.54%	33.65%
5	Netherlands	5 032 830	4 093 890	2 801 098	1 639 583	17.13M	29.38%	23.9%	16.35%
6	Saudi Arabia	10 044 842	9 419 488	12 760 979	10 081 329	34.81M	28.86%	27.06%	36.65%
7	Kuwait	1 075 914	818 069	1 265 560	933 664	4.27M	25.2%	19.16%	29.63%
8	Turkey	14 398 181	12 390 300	19 020 753	9 449 156	84.34M	17.07%	14.69%	22.55%
9	France	10 534 433	8 907 640	6 017 733	3 425 823	65.27M	16.14%		9.22%
10	Australia	3 988 989	2 581 455	2 503 351	2 498 393	25.50M	15.64%		9.82%

Рисунок 5 – Загальна кількість завантажень VPN у світі
станом на 2023 рік [3]

У 2023 році Україна у цьому списку посіла 33 місце у світовому рейтингу використання VPN. Кількість завантажень склала 3 975 823 – 9,09% населення нашої країни завантажили VPN-додаток.

Висновки. Технологія VPN значно спрощує дотримання вимог інформаційної безпеки. Однак в Україні дана технологія поки що на початкових етапах свого розвитку.

Інформаційні джерела

1. Daniel Petri. Understanding VPN Remote Access Mechanism. URL: https://petri.com/understanding-vpn-remote-access-mechanism

2. Douglas Crawford. OpenVPN over TCP vs. UDP: what is the difference, and which should I choose? URL: https://www.bestvpn.com/blog/7359/openvpn-tcp-vs-udp-difference-choose/

3. Веб-сайт "Dev.ua". URL: https://dev.ua/news/vpn-2023-1705920849.

4. Полотай О. І., Дубик А.-О. Ю. Особливості захисту інформації в комп'ютерних мережах. "Світ наукових досліджень" (матеріали Міжнародної мультидисциплінарної наукової інтернет-конференції (м. Тернопіль, Україна, м. Ополе, Польща, 24–25 жовтня 2023 р.). Вип. 23. – С. 291–292.

УДК 004.838

БРАНДМАУЕРИ ТА ЇХ ВИКОРИСТАННЯ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

Василь ЛУЧИК
Іван ГУМЕНЮК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *In today's digital world, firewalls are an important element of cybersecurity, providing protection for networks and devices from cyberattacks and unauthorized access. They perform the functions of filtering network traffic, controlling access, detecting threats and preventing the penetration of malicious software. Firewalls can be software or hardware, and their latest versions combine in-depth content analysis and integration with intrusion prevention systems (IPS). The use of such systems allows you to effectively respond to threats, create secure connections (VPNs) and ensure the confidentiality of information. A comprehensive approach involving firewalls and other cybersecurity measures helps reduce risks and increase data protection in networks at different levels.*

Keywords: *firewall, cybersecurity, network protection, traffic filtering, access control, IPS, VPN, cyber threats, NAT, information security.*

Анотація. *У сучасному цифровому світі брандмауери є важливим елементом кібербезпеки, забезпечуючи захист мереж і пристроїв від кібератак та несанкціонованого доступу. Вони виконують функції фільтрації мережевого трафіку, контролю доступу, виявлення загроз і запобігання проникненню шкідливого програмного забезпечення. Брандмауери можуть бути програмними або апаратними, а їх новіт-*

ні версії поєднують поглиблений аналіз контенту та інтеграцію з системами запобігання вторгненням (IPS). Використання таких систем дозволяє ефективно реагувати на загрози, створювати захищені з'єднання (VPN) і забезпечувати конфіденційність інформації. Комплексний підхід із залученням брандмауерів та інших заходів кібербезпеки сприяє зниженню ризиків і підвищенню захисту даних у мережах різного рівня.

Ключові слова: *брандмауер, кібербезпека, мережевий захист, фільтрація трафіку, контроль доступу, IPS, VPN, кіберзагрози, NAT, інформаційна безпека.*

У сучасну епоху цифрових технологій кібербезпека стала важливим аспектом діяльності як окремих користувачів, так і організацій. Однією з основних загроз є несанкціонований доступ до даних та кібератаки, які можуть спричинити значні фінансові втрати та порушення приватності. Для захисту інформаційних систем застосовуються різні методи та засоби, і брандмауери є одним із ключових інструментів у цьому процесі.

Важливість брандмауерів у забезпеченні кібербезпеки полягає у їх здатності захищати конфіденційність користувачів, запобігаючи несанкціонованому доступу до особистих даних, таких як паролі та фінансова інформація.

У комп'ютерних мережах брандмауер (фаєрвол) виконує функцію виявлення та блокування мережевого трафіку згідно з попередньо заданими або динамічними правилами. Вони забезпечують захист мереж і пристроїв від можливих атак кіберзлочинців, які можуть заражати пристрої та використовувати їх у зловмисних цілях [1].

Термін "firewall" походить від англійської мови та означає протипожежну стіну, яка запобігає поширенню вогню та знижує ризики для людей. У сфері мережевої безпеки фаєрвол є програмним або апаратним засобом, що діє як бар'єр між захищеними та неперевіреними мережами або їх частинами. Основною метою брандмауера є фільтрація потенційно небезпечного та шкідливого контенту й з'єднань [1].

Програмні брандмауери працюють безпосередньо на окремих пристроях, таких як комп'ютери чи сервери, забезпечуючи їх захист від мережевих загроз. Їх можна легко налаштовувати та оновлювати, але це може призвести до використання системних ресурсів, що іноді впливає на продуктивність. Апаратні брандмауери – це окремі пристрої, розташовані між мережею та її підключенням до Інтернету, що забезпечують більш високий рівень безпеки. Однак вони є дорожчими та складнішими в обслуговуванні порівняно з програмними рішеннями [2].

Брандмауери нового покоління мають особливу спеціалізацію на захисті від шкідливих програм і атак на рівні додатків. У поєднанні з системами запобігання вторгненням (IPS) вони можуть миттєво реагувати на загрози, виявляючи та нейтралізуючи їх у межах мережі. Такі брандмауери діють відповідно до встановлених політик, забезпечуючи надійний захист мережі,

і проводять аналіз для виявлення потенційно небезпечної активності, блокуючи шкідливе ПЗ. Використання брандмауерів у системі безпеки дозволяє створити політики для контролю та фільтрації трафіку, що надходить і виходить із мережі [3].

Основні функції брандмауерів включають:

Фільтрацію трафіку: брандмауери аналізують та відсіюють пакети даних при вході та виході з мережі, дозволяючи або блокуючи їх на основі встановлених правил.

Контроль доступу: вони визначають, які програми, служби та пристрої можуть мати доступ до мережі, забезпечуючи захист конфіденційних ресурсів.

Виявлення загроз: деякі брандмауери можуть знаходити та запобігати загрозам, таким як віруси, зловмисне програмне забезпечення або підозріла активність [4].

Існують різні типи брандмауерів, що відрізняються методами фільтрації трафіку. Перший тип – це пакетні фільтри, що аналізують основні дані пакета (джерело, призначення, порт і протокол) і порівнюють їх із заданими правилами. Друге покоління додає контроль стану з'єднань, що дозволяє відстежувати початок і активність з'єднання. Брандмауери третього покоління використовують фільтрацію на всіх рівнях моделі OSI, включаючи прикладний рівень, що дозволяє їм розпізнавати програми та протоколи, такі як FTP та HTTP, і виявляти спроби обходу через дозволені порти або несанкціоноване використання протоколу. Новіші брандмауери, відомі як брандмауери наступного покоління (NGFW), поєднують ці методи з поглибленим аналізом контенту, що допомагає визначити потенційно небезпечний трафік на основі бази даних [1].

Таблиця 1.

Відмінності між брандмауерами та антивірусами

Параметр	*Брандмауер*	*Антивірус*
Основна функція	Контроль та моніторинг мережевого трафіку, блокування небажаних з'єднань	Виявлення, запобігання та видалення шкідливого ПЗ
Рівень захисту	Працює на мережевому рівні, контролює дані, що надходять і виходять з мережі	Працює на рівні файлів і системи, сканує файли та програми
Запобігання атакам	Захищає від несанкціонованого доступу, фільтрує підозрілу активність у мережі	Захищає від відомих вірусів, троянів, шпигунських програм
Спосіб роботи	Фільтрує мережевий трафік за заданими правилами	Сканує та перевіряє файли та програми на наявність загроз
Взаємодія з користувачем	Потребує налаштування правил для блокування або дозволу трафіку	Переважно працює у фоновому режимі та автоматично реагує на загрози

Приклади загроз, що запобігаються	DDoS-атаки, спроби несанкціонованого доступу	Віруси, руткіти, програми-вимагачі, шпигунські програми
Додаткові можливості	Інтеграція з VPN, системами запобігання вторгненням (IPS), фільтрація URL	Розширений захист електронної пошти, захист під час серфінгу в Інтернеті
Режим роботи	Може діяти як програмне забезпечення або апаратний пристрій	Переважно програмне забезпечення

Брандмауери виконують важливі функції на мережевому рівні, такі як трансляція мережевих адрес (NAT) та створення віртуальних приватних мереж (VPN). NAT забезпечує приховування або зміну внутрішніх IP-адрес клієнтів і серверів, які можуть бути у "приватному діапазоні адрес" згідно з RFC 1918, на загальнодоступні IP-адреси. Це сприяє збереженню обмеженої кількості IPv4-адрес і захищає від мережевої розвідки, оскільки внутрішні IP-адреси залишаються прихованими від Інтернету. У свою чергу, VPN розширює приватну мережу через загальнодоступну, створюючи захищений тунель, часто із шифруванням, який забезпечує захист вмісту пакетів під час їх передавання через Інтернет. Це дозволяє користувачам безпечно передавати й отримувати дані через спільні або публічні мережі [3].

Висновки. Отже, брандмауери відіграють важливу роль у забезпеченні кібербезпеки як для організацій, так і для індивідуальних користувачів. Вони створюють першу лінію захисту, контролюючи та фільтруючи вхідний і вихідний мережевий трафік, запобігаючи несанкціонованому доступу та блокуючи потенційно небезпечну активність. Завдяки сучасним брандмауерам, що інтегрують систему запобігання вторгненням (IPS) і мають розширені функції моніторингу та аналізу, стає можливим швидке реагування на загрози та їх нейтралізація. Використання брандмауерів у комплексі з іншими заходами кібербезпеки забезпечує більш високий рівень захисту даних і зменшує ризики кібератак. Це робить їх невід'ємною частиною стратегії безпеки в сучасному цифровому середовищі.

Інформаційні джерела

1. Брандмауер. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/brandmauer/?srsltid=AfmBOoq-L7h6YDq_BHvMRNG_CHNECOpPjCf5DtHFK9AJxlgNTT3IvGpk (дата звернення 14.11.2024).

2. Types of Firewalls for Cybersecurity. URL: https://www.coursera.org/articles/types-of-firewalls (дата звернення 14.11.2024).

3. What is a Firewall? URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/ (дата звернення 14.11.2024).

4. What is a Firewall? A Guide to Network Security and Safety. URL: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall (дата звернення 14.11.2024).

УДК 004.838

БЕЗПЕКА ЕЛЕКТРОННОЇ ПОШТИ: МЕТОДИ ЗАХИСТУ ВІД СПАМУ ТА ШКІДЛИВИХ ВКЛАДЕНЬ

Віталій СВІТЛИЧНИЙ
Ярослав КОЛОДА
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *Email remains one of the most important means of communication, but at the same time it is a source of significant cyber threats, including spam, malicious attachments and phishing attacks. Spam is not only inconvenient, but can also be used to spread malware or steal confidential information. Malicious attachments pose a serious threat that can damage devices or compromise user data. To ensure email security, it is important to apply a comprehensive approach: install antivirus software, configure spam filters, implement multi-factor authentication and train users to recognize threats. Regular updates of programs and the use of modern technologies can minimize the risks associated with email.*

Keywords: *email, cybersecurity, spam, malicious attachments, phishing, antivirus, spam filter, data protection, multi-factor authentication.*

Анотація. *Електронна пошта залишається одним із найважливіших засобів комунікації, але водночас є джерелом значних кіберзагроз, зокрема спаму, шкідливих вкладень і фішингових атак. Спам не лише викликає незручності, але й може використовуватися для поширення шкідливих програм або викрадення конфіденційної інформації. Шкідливі вкладення становлять серйозну загрозу, здатну пошкодити пристрої або скомпрометувати дані користувачів. Для забезпечення безпеки електронної пошти важливо застосовувати комплексний підхід: встановлювати антивірусне програмне забезпечення, налаштовувати спам-фільтри, впроваджувати багатофакторну автентифікацію та навчати користувачів розпізнавати загрози. Регулярне оновлення програм і застосування сучасних технологій дозволяють мінімізувати ризики, пов'язані з електронною поштою.*

Ключові слова: *електронна пошта, кібербезпека, спам, шкідливі вкладення, фішинг, антивірус, спам-фільтр, захист даних, багатофакторна автентифікація.*

Електронна пошта є одним із найпоширеніших засобів комунікації як у приватному, так і в професійному середовищі. Однак з її популярністю зростає і кількість загроз, пов'язаних із використанням електронної пошти, серед яких спам, шкідливі вкладення та фішингові атаки займають провідні позиції. Спам, що складає значну частину всього електронного листування, може бути не тільки набридливим, а й небезпечним, оскільки часто використовується для розповсюдження шкідливих програм або обману користувачів із метою отримання конфіденційної інформації.

Шкідливі вкладення у листах становлять додаткову загрозу, оскільки можуть містити віруси, трояни та інші види шкідливого програмного забезпечення, здатні завдати значної шкоди комп'ютерним системам і даним. Зважа-

ючи на постійний розвиток технологій та вдосконалення методів кібератак, питання забезпечення безпеки електронної пошти стає особливо актуальним.

Спам – це масове надсилання повідомлень без згоди отримувача через електронну пошту, месенджери, соціальні мережі та SMS, а також повторювані рекламні дзвінки. *Наприклад*, бізнес може займатися спамом, коли розсилає шаблонні повідомлення про акції, знижки або будь-яку рекламу, спрямовану на збільшення продажів. Хоча такий метод просування зазвичай більше шкодить репутації бренду, ніж підвищує відсоток конверсії, він залишається популярним через можливість охопити широку аудиторію з мінімальними витратами часу та грошей. Однак, крім невинних, хоча й непотрібних повідомлень, зловмисники можуть використовувати електронні листи для завдання шкоди, викрадення даних банківських рахунків або іншої конфіденційної інформації [1].

Відкриття вкладень у електронних листах може нести потенційну загрозу для вашого пристрою, адже вони можуть містити віруси чи інше шкідливе програмне забезпечення, яке здатне виконувати небажані дії без вашого відома. Якщо ви отримали вкладення, яке викликає сумніви, важливо знати, як забезпечити безпеку свого пристрою. По-перше, ніколи не відкривайте вкладення, якщо не впевнені у його джерелі або вмісті. Відкриття підозрілих файлів може призвести до зараження пристрою вірусами або іншими шкідливими програмами. Для захисту вкладень електронної пошти рекомендується встановлювати та регулярно оновлювати антивірусне програмне забезпечення. Такі програми здатні виявляти шкідливі файли та блокувати їх ще до моменту відкриття. Крім того, варто бути обережним під час завантаження файлів з інтернету та обов'язково перевіряти їх на наявність вірусів чи шкідливого ПЗ перед відкриттям [2].

Дуже часто електронна пошта стає каналом для поширення спаму та інфікованих повідомлень зі шкідливим програмним забезпеченням. З метою захисту від великої кількості небажаних та небезпечних листів багато поштових серверів використовують "чорні" списки відомих відправників спаму та фішингу. Додатково можна застосовувати фільтрацію повідомлень за типом вкладень або дозволяти отримання лише від перевірених джерел. Щоб забезпечити безпеку своїх користувачів, багато організацій перевіряють повідомлення на наявність шкідливих програм і вірусів перед їх поширенням через мережу [3].

Самостійно налаштувати поштову скриньку для боротьби зі спамом може бути складно. Щоб частково уникнути спамових повідомлень, можна скористатися наступними методами:

Не відповідайте на спам. Якщо з теми листа зрозуміло, що це спам, навіть не відкривайте його. Якщо відкрили, видаліть лист негайно, не переходячи за посиланнями та не завантажуючи вкладення. Завжди уважно перевіряйте адреси відправників, адже такі листи можуть маскуватися під важливі повідомлення від магазинів чи банків.

Використовуйте розширення або програми для захисту від спаму. Окрім вбудованих спам-фільтрів, додатково можна застосовувати сторонні програмні фільтри та розширення.

Не поширюйте свою електронну адресу. Не публікуйте її на загальнодоступних ресурсах та уникайте використання для реєстрації. Спамери часто використовують спеціальні програми для автоматичного збору адрес [4].

Оскільки зловмисники постійно змінюють свої методи, щоб уникнути виявлення, спам-фільтри повинні адаптуватися, щоб відповідати новим загрозам. Одним із способів протистояння сучасним формам спаму є регулярне оновлення спам-фільтра. Переконайтеся, що на вашому поштовому сервері або захищеному електронному шлюзі встановлена остання версія програмного забезпечення. Якщо ви використовуєте SpamAssassin або іншу антивірусну службу, переконайтеся, що вона налаштована на автоматичне отримання оновлень спам-фільтра. У MDaemon та SecurityGateway є функції для регулярної перевірки таких оновлень [5].

Висновки. У підсумку, безпека електронної пошти є критичним аспектом сучасного цифрового середовища, адже спам та шкідливі вкладення можуть завдати значної шкоди як окремим користувачам, так і організаціям. Для зниження ризиків важливо дотримуватися комплексного підходу, який включає використання антивірусного програмного забезпечення, налаштування ефективних спам-фільтрів, підвищення обізнаності користувачів про основні ознаки фішингових та шкідливих повідомлень, а також впровадження багатофакторної автентифікації. Своєчасне оновлення програмного забезпечення та дотримання простих правил безпеки можуть значно зменшити ризик успішних атак. Захист від спаму та шкідливих вкладень – це не лише технічне завдання, а й важлива складова загальної культури безпеки кожного користувача інтернету.

Інформаційні джерела

1. Спам на електронній пошті: види листів та методи боротьби з ними. URL: https://web-promo.ua/ua/blog/spam-na-elektronnij-poshti-vidi-listiv-ta-metodi-borotbi-z-nimi/# (дата звернення 15.11.2024).

2. Вкладення електронної пошти та віруси – як захистити себе від небезпеки. URL: https://mediacom.com.ua/vkladennya-elektronnoi-poshti-ta-virusi-yak-zalishitisya-v-bezpetsi/ (дата звернення 15.11.2024).

3. Безпека пошти: основні рекомендації для захисту скриньок від онлайн-загроз. URL: https://www.eset.com/ua/about/newsroom/press-releases/security-tips/bezopasnost-pochty-vneshniye-i-vnutrenniye-faktory-zashchity-pochty/?srsltid=AfmBOopJ6bU5f2NTLy6E1Sw4iIv0cYkAjULqlaFTMoqNbCeJcqDz8Z0W (дата звернення 15.11.2024).

4. Як захистити пошту від спаму та вірусів. URL: https://www.nspace.ua/info/yak-zahistiti-poshtu-vid-spamu-ta-virusiv (дата звернення 15.11.2024).

5. Top 9 Email Security Tips to Protect Against Spam, Phishing & Malware. URL: https://blog.mdaemon.com/top-9-email-security-tips-to-protect-against-spam-phishing-malware (дата звернення 15.11.2024).

УДК 004.7

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ЗАХИСТУ ВІД АТАК VLAN HOPPING

Сніжана ОРИНИК
Орест ПОЛОТАЙ
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The peculiarities of the VLAN hopping attack are described, how malicious criminals operate on virtual local networks. New rules have been introduced to combat VLAN hopping attacks.*
Keywords: *information security, virtual private network, VLAN hopping attack.*

Анотація. *Описано особливості атаки VLAN hopping, які зловмисники здійснюють на віртуальні локальні мережі. Наведено перелік правил для запобігання атакам VLAN hopping.*
Ключові слова: *інформаційна безпека, віртуальна приватна мережа, атака VLAN hopping.*

Віртуальні мережі в даний час входять в число найважливіших стратегічних напрямків майже всіх найбільших виробників мережевого устаткування. Звичайна мережа з роздільним середовищем передачі не може забезпечити велику пропускну здатність. І це було пов’язано з появою мультимедійних додатків, кількість яких постійно збільшується а також клієнт-серверних додатків. Саме ці передумови спонукали розробників створити різні технології захисту і поділу інформації всередині існуючої мережі. Однією з таких технологій є віртуальні локальні обчислювальні мережі (VLAN).

VLAN (Virtual Local Area Network) – топологічна, або віртуальна, локальна мережа. VLAN – це логічне комбінування деякого числа кінцевих станцій в одному сегменті (широкомовному домені) на канальному рівні, навіть якщо вони фізично підключені до різних комутаторів. VLAN дозволяє повністю ізолювати трафік групи вузлів від решти мережі. Даний вид організації мережі дозволяє забезпечувати досить потужні бар’єри на шляху помилкового трафіку при його передачі з однієї мережі в іншу, таким чином забезпечуючи захист інформаційних потоків в межах окремих доменів.

Однак мережі VLAN також мають вразливі місця та можуть підпадати під загрози інформаційної безпеки. Однією з таких загроз є атака VLAN hopping.

VLAN hopping – це експлуатація вразливості у комп’ютерних мережах, що дозволяє зловмиснику обминути передбачені обмеження віртуальних локальних мереж – VLAN. Це метод, який використовується хакерами для

несанкціонованого доступу до мережевих ресурсів шляхом маніпулювання конфігураціями VLAN та використання вразливостей у комутаторах.

Атаки VLAN hopping експлуатують різні вразливості в мережевих комутаторах і методах конфігурації VLAN. Ось деякі поширені методи, що використовуються в VLAN hopping:

Подвійне тегування: У цій техніці зловмисник відправляє кадр із двома тегами 802.1Q. Перший тег – це власний тег VLAN зловмисника, а другий тег – тег VLAN цільової VLAN. Таким чином, зловмисник дурить комутатор, змушуючи його переслати кадр у непризначену VLAN.

Підробка комутатора: Підробка комутатора – це інший метод, який використовується в атаках VLAN hopping. Зловмисник отримує доступ до управління VLAN, підробляючи оголошення комутатора. Це дозволяє зловмиснику перехоплювати та модифікувати мережевий трафік, потенційно отримуючи несанкціонований доступ до конфіденційної інформації.

Експлуатація протоколу динамічного транкінгу (DTP): DTP – це пропрієтарний протокол від Cisco, який використовується для узгодження транкових з'єднань між комутаторами. Шляхом експлуатації DTP зловмисник може переконати комутатор змінити його режим на транкінг. Це дає зловмиснику доступ до кількох VLAN, оминаючи передбачені обмеження VLAN.

Щоб запобігти атакам VLAN hopping та підвищити безпеку вашої мережі, можна реалізувати наступні заходи:

1. Вимкнення портів, що не використовуються: потрібно відключити всіх порти комутатора, які не використовуються, щоб запобігти фізичному доступу зловмисника до мережі через ці порти. Відключаючи порти, що не використовуються, зменшується поверхня атаки і обмежуються потенційні точки входу.

2. Вимкнення протоколу динамічного транкінгу (DTP): Необхідно налаштувати порти комутатора вручну як порти доступу, а не транкові порти, і вимкнути DTP. Таким чином, виключається ризик експлуатації DTP, який часто використовується в атаках VLAN hopping.

3. Реалізація списків контролю доступу VLAN (VACL): VACL забезпечують додатковий рівень безпеки, що дозволяє вам контролювати потік трафіку між VLAN. Посилюючи правила контролю доступу, можна запобігти несанкціонованому спілкуванню між VLAN і зменшити ризик VLAN hopping.

4. Увімкнення безпеки портів: безпека портів дозволяє обмежувати кількість MAC-адрес, що допускаються на конкретний порт комутатора. Налаштувавши безпеку портів, можна запобігти підключенню несанкціонованих пристроїв до мережі та обмежити потенційну дію атак VLAN hopping.

5. Регулярне оновлення прошивки комутатора: необхідно утримувати свої мережеві комутатори в актуальному стані, встановлюючи останні прошивки та патчі безпеки. Це гарантує, що будь-які відомі вразливості, які можуть бути використані для VLAN hopping, будуть усунені та нейтралізовані.

Інформаційні джерела

1. Веб-сайт “Vpnunlimited.com/”. URL: https://www.vpnunlimited.com/
2. Полотай О. І., Дубик А.-О. Ю. Особливості захисту інформації в комп’ютерних мережах. “Світ наукових досліджень” (матеріали Міжнародної мультидисциплінарної наукової інтернет-конференції (м. Тернопіль, Україна, м. Ополе, Польща, 24–25 жовтня 2023 р.). Вип. 23. – С. 291–292.
3. Методи і технології захисту комп’ютерних мереж (фізичний та канальний рівні). URL: https://ela.kpi.ua/server/api/core/bitstreams/e5c73b24-058a-42d8-bd2d-03a17e2c7c9a/content.

УДК 004.8:354

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОТИДІЇ ІНТЕРНЕТ ПІРАТСТВУ

Дмитро КУРИЛО
Віталій СВІТЛИЧНИЙ
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам’янець-Подільський, Україна.

Abstract*. The problem of Internet piracy, which causes significant financial losses to creators of digital content and affects the quality of products available to consumers, is studied. The role of artificial intelligence (AI) in combating piracy is considered, in particular the use of machine learning algorithms, big data analysis and cryptography. Examples of successful application of AI for automatic detection of illegal content, identification of pirated resources and development of innovative protection technologies such as unique “watermarks” are described. A conclusion was made about the prospects of implementing AI as an effective tool in the fight against Internet piracy and its potential for creating a safe digital environment.*

Keywords*: Internet piracy, artificial intelligence, copyright, machine learning, digital content, big data, cryptography, information protection.*

Анотація. *Досліджено проблему інтернет-піратства, що завдає значних фінансових збитків творцям цифрового контенту та впливає на якість продуктів, доступних споживачам. Розглядається роль штучного інтелекту (ШІ) у протидії піратству, зокрема використання алгоритмів машинного навчання, аналізу великих даних та криптографії. Описано приклади успішного застосування ШІ для автоматичного виявлення нелегального контенту, ідентифікації піратських ресурсів та*

розробки інноваційних технологій захисту, таких як унікальні "водяні знаки". Зроблено висновок про перспективність впровадження ШІ як ефективного інструмента у боротьбі з інтернет-піратством та його потенціал для створення безпечного цифрового середовища.

Ключові слова: *інтернет-піратство, штучний інтелект, авторське право, машинне навчання, цифровий контент, великі дані, криптографія, захист інформації.*

Інтернет-піратство стало однією з найсерйозніших загроз для індустрій, що створюють цифровий контент, включаючи музичну, кіноіндустрію, програмне забезпечення та видавничий бізнес. Поширення нелегальних копій фільмів, музики, програм та інших продуктів завдає величезних фінансових збитків правовласникам та творцям [1]. Це також впливає на споживачів, оскільки піратські копії часто мають низьку якість та можуть містити шкідливе програмне забезпечення. Однак, стрімкий розвиток ШІ відкриває нові можливості для ефективної боротьби з інтернет-піратством. Використання ШІ для протидії цьому явищу може значно змінити правила гри, забезпечуючи більш точне виявлення та видалення нелегального контенту з мережі.

Існує кілька способів, як штучний інтелект може бути використаний для протидії інтернет-піратству. По-перше, алгоритми машинного навчання можуть бути використані для автоматичного виявлення піратського контенту. *Наприклад*, нейронні мережі можуть аналізувати відео та аудіофайли, порівнюючи їх з легальними копіями, щоб ідентифікувати порушення авторських прав. Цей підхід вже застосовується деякими великими компаніями, такими як YouTube, які використовують систему Content ID для автоматичного виявлення та монетизації нелегального контенту.

По-друге, штучний інтелект може допомогти в аналізі великих обсягів даних для виявлення піратських сайтів та платформ. Використовуючи технології обробки природної мови (NLP) та аналізу великих даних, ШІ може виявляти закономірності та аномалії, що свідчать про існування піратських ресурсів [2]. Це дозволяє правоохоронним органам та компаніям вчасно реагувати на нові загрози та блокувати доступ до таких ресурсів.

По-третє, штучний інтелект може використовуватись для розробки нових методів захисту контенту. *Наприклад*, криптографічні алгоритми на основі ШІ можуть створювати унікальні "водяні знаки", які важко підробити або видалити [3]. Це дозволяє відстежувати походження кожної копії цифрового контенту та швидко виявляти його нелегальне розповсюдження. Крім того, ШІ може бути використаний для вдосконалення технологій цифрових підписів та автентифікації, що робить процес захисту контенту більш надійним та ефективним.

Висновки. Використання штучного інтелекту для протидії інтернет-піратству є перспективним напрямком, який може суттєво зменшити обсяги нелегального розповсюдження цифрового контенту. Завдяки можливостям машинного навчання, обробки великих даних та криптографії, ШІ дозволяє

більш ефективно виявляти, відстежувати та захищати контент від піратства. Це не лише допоможе зберегти фінансові ресурси творців контенту, але й забезпечить споживачам доступ до якісного та безпечного продукту. У майбутньому подальший розвиток технологій штучного інтелекту може стати ключовим елементом у боротьбі з інтернет-піратством, забезпечуючи більш надійний та справедливий цифровий простір для всіх учасників.

Інформаційні джерела

1. Інтернет піратство. Українська Антипіратська Асоціація. URL: https://apo.kiev.ua/internet.phtml (дата звернення: 24.10.2024).

2. Що таке НЛП та як воно працює?. MC.today, Media for Creators. URL: https://mc.today/uk/shho-take-nejrolingvistichne-programuvannya-ta-yak-vono-pratsyuye/ (дата звернення: 24.10.2024).

3. Учасники проектів Вікімедіа. Цифровий водяний знак – Вікіпедія. URL: https://uk.wikipedia.org/wiki/Цифровий_водяний_знак (дата звернення: 24.10.2024).

УДК 004.056

ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ МІЖНАРОДНОЇ РЕКЛАМНОЇ АГЕНЦІЇ В УМОВАХ ДЕЦЕНТРАЛІЗОВАНОГО СЕРЕДОВИЩА

Владислав НАЗАРОВ
Національний університет "Одеська політехніка", м. Одеса, Україна.

Abstract. *International advertising agencies operate in virtual environments without physical offices, relying on cloud services, BYOD policies, and platforms like Google Drive, Salesforce, and Slack. This increases the risks of phishing attacks, data breaches, and intellectual property theft, necessitating a comprehensive, multi-layered approach to cybersecurity and proactive threat monitoring.*

Keywords: *Zero Trust Architecture, intellectual property, SIEM, advertising agency.*

Анотація. *Міжнародні рекламні агенції працюють у віртуальному середовищі без фізичних офісів, використовуючи хмарні середовища, політику BYOD та різноманітні системи, зокрема Google Drive, Salesforce і Slack. Це підвищує ризики фішингових атак, витоків даних і крадіжки інтелектуальної власності, що вимагає комплексного багаторівневого підходу до кібербезпеки.*

Ключові слова: *Zero Trust Architecture, інтелектуальна власність, SIEM, кібербезпека, рекламна агенція.*

Основні загрози в умовах роботи міжнародної рекламної агенції

Згідно з даними Verizon Data Breach Investigations Report 2023 [1], людський фактор залишається основною причиною порушень кібербезпеки, від-

повідаючи за 68% інцидентів (рис. 1), включаючи атаки соціальної інженерії та ненавмисні помилки працівників. При цьому 14% атак пов'язані з експлуатацією технічних вразливостей, що свідчить про зростання їхньої небезпеки порівняно з попередніми роками. Ще 15% інцидентів викликані діями третіх сторін, таких як постачальники або адміністратори даних. Фінансово мотивовані атаки, зокрема ті, що використовують програмне забезпечення-вимагач (ransomware), становлять 62% від усіх зафіксованих інцидентів.

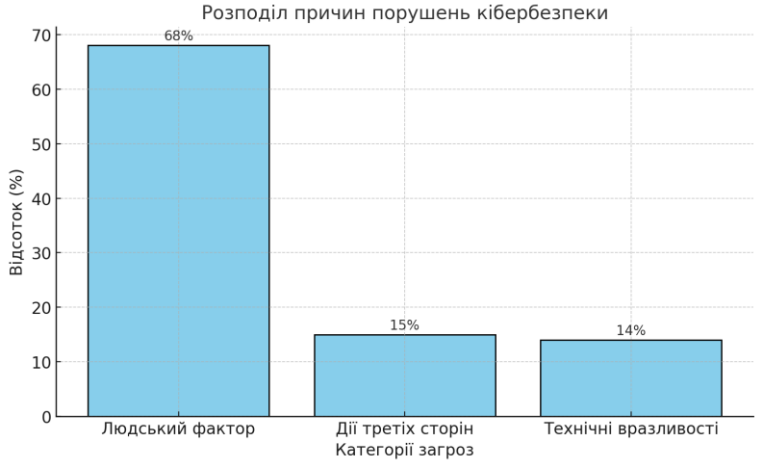


Рисунок 1 – Графік розподілу відсотків порушень кібербезпеки

Ці дані наголошують на необхідності впровадження сучасних підходів до кіберзахисту. Зокрема, аналіз поведінки користувачів та пристроїв UEBA (User and Entity Behavior Analytics) дозволяє виявляти аномалії у взаємодії з системами, такі як незвичні дії користувачів чи підозріла активність пристроїв. UEBA є важливою складовою систем управління інформаційною безпекою SIEM (Security Information and Event Management), що охоплюють збір, аналіз і моніторинг даних про події в системі. SIEM забезпечує централізовану платформу для виявлення загроз, швидкого реагування та підтримки цілісності мережі.

Компрометація облікових записів через фішингові атаки. Зловмисники використовують соціальну інженерію для надсилання підроблених електронних листів чи повідомлень, що містять посилання на фальшиві сторінки для входу. Отримавши облікові дані, вони отримують доступ до корпоративних систем, таких як CRM або хмарні сервіси, і можуть викрасти клієнтські бази чи інші конфіденційні дані.

Крадіжка інтелектуальної власності. Невдоволені співробітники або зловмисники можуть копіювати рекламні концепції, відео чи графічні файли

з платформ, зокрема Adobe Creative Cloud, і передавати їх конкурентам або використовувати для особистої вигоди.

Викрадення пристроїв. У разі крадіжки особистих пристроїв працівників, які зберігають активні сесії доступу до хмарних сервісів, зловмисники можуть використати їх для несанкціонованого доступу до корпоративних систем.

Атаки на хмарні сервіси. Зловмисники можуть намагатися зламати хмарні сховища (Google Drive, Dropbox) для викрадення інформації, використовуючи методи грубої сили або скомпрометовані паролі.

Інсайдерські загрози. Співробітники, які мають обмежені знання кібергігієни або умисно намагаються завдати шкоди, можуть спричинити витоки даних, змінити критичну інформацію або відкрити доступ стороннім особам.

Політика "Принеси свій пристрій" (BYOD) та її ризики

Політика "Bring Your Own Device" (BYOD) дозволяє працівникам використовувати власні пристрої (ноутбуки, смартфони, планшети) для доступу до корпоративних систем. Це зручно для міжнародної рекламної агенції, яка працює у децентралізованому середовищі, адже співробітники можуть працювати з будь-якого місця, використовуючи персональне обладнання. Однак BYOD створює низку таких ризиків.

1. Різноманітність пристроїв. Кожен пристрій має свої характеристики, рівень захищеності та можливі вразливості (*наприклад*, існує суттєва різниця між оперативними системами Android та iOS).

2. Незахищені мережі. Співробітники можуть підключатися до відкритих Wi-Fi мереж, які легко можуть бути скомпрометовані зловмисниками для перехоплення пакетів даних.

3. Втрата або викрадення пристрою. Це може надати зловмисникам доступ до корпоративних даних та систем через збережені на пристроях логіни та паролі.

4. Відсутність централізованого управління. Особисті пристрої можуть не відповідати загальним корпоративним політикам безпеки.

Складові захисту для BYOD в умовах міжнародної рекламної агенції

1. Управління пристроями. Впровадження Mobile Device Management (MDM) для моніторингу та забезпечення безпеки пристроїв. *Наприклад,* Jamf або Microsoft Intune дозволяють дистанційно контролювати доступ до корпоративних даних, віддалено очищувати дані у разі викрадення пристрою.

2. Вимоги до пристроїв. Співробітники повинні встановлювати корпоративне програмне забезпечення, зокрема VPN для захищеного з'єднання та інструменти шифрування (*наприклад*, BitLocker для Windows або FileVault для macOS).

3. Навчання персоналу. Обов'язкові тренінги з кібергігієни для розпізнавання фішингових атак, налаштування безпечних мереж і створення надійних паролів.

4. Контроль доступу. Використання багатофакторної автентифікації (MFA) та обмеження доступу до корпоративних даних на основі географічного розташування (геофенсінг).

5. Реагування на інциденти. Політика повинна передбачати чіткий план дій у разі викрадення пристрою. *Наприклад*:

– відключення пристрою від корпоративної мережі та ресурсів;

– дистанційне видалення даних із пристрою через функціонал MDM;

– проведення аудиту безпеки для визначення можливих фактів витоків чутливих даних, причин, можливих сценаріїв та їхніх фігурантів.

Аспекти технічного середовища та рекомендації для захисту інформації

Zero Trust Architecture (ZTA) – це елемент комплексного підходу до кібербезпеки, який добре підходить для децентралізованих організацій, якими є міжнародні рекламні чи маркетингові агенції. Модель ZTA (рис. 2) передбачає повну відсутність довіри до пристроїв та користувачів за замовчуванням, що забезпечує постійний контроль кожного запиту на доступ до ресурсів. Інструменти на кшталт ZScaler та Cloudflare Access виконують динамічну перевірку пристроїв, їхньої локалізації та активності користувача, що знижує ризик компрометації даних.

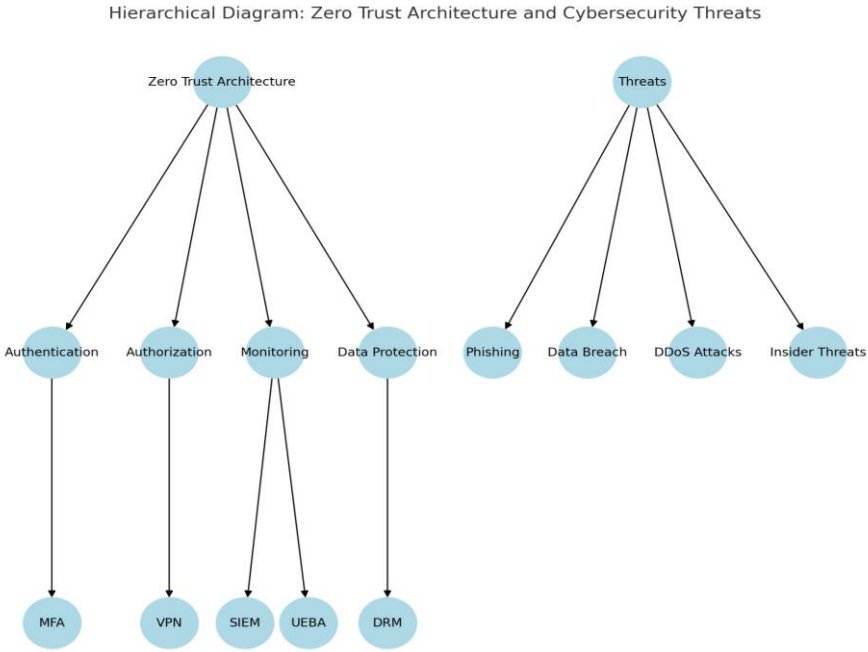


Рисунок 2 – Ієрархічна структура архітектури з нульовою довірою

Реалізація заходів безпеки (таб. 1) починається з аудиту доступу та ідентифікації на основі принципу найменшого доступу (PoLP). Це дозволяє мінімізувати ризики, пов'язані з інсайдерськими загрозами (навмисно влаштовані витоки даних). Регулярні тестування на проникнення допомагають виявляти вразливості у хмарних середовищах, а SIEM-системи забезпечують швидке реагування на кіберінциденти.

Таблиця 1.

Категорії захисту та технологічні рішення

Категорія захисту	*Технологічні рішення*
Захист облікових даних	Багатофакторна автентифікація (Google Authenticator, Duo Security), менеджери паролів (1Password, LastPass)
Моніторинг активності	UEBA-системи (Splunk, Sumo Logic), SIEM-системи (IBM QRadar, Elastic Security), аудит дій у хмарних платформах (Audit Logs)
Захист інтелектуальної власності	DRM (Digital Rights Management) рішення (Fasoo, Seclore), моніторинг змін у файлах і конфігураціях хмарних платформ
Інцидент-менеджмент	Віддалене вилучення данних з пристроїв (Prey, Find My Device), впровадження Zero Trust Architecture (ZScaler, Cloudflare Access)

Важливим елементом є впровадження UEBA-систем, які аналізують поведінку користувачів та пристроїв для виявлення аномалій. Це дозволяє швидко виявляти підозрілу активність, *наприклад*, спроби масового завантаження даних або доступ із невідомих географічних регіонів, забезпечуючи проактивний захист.

Особливу увагу слід приділити навчанню працівників основам кібергігієни: від уникнення фішингових атак до роботи в захищених мережах (таб. 2). У разі викрадення пристрою повинні застосовуватися заходи для миттєвого блокування доступу та видалення конфіденційних даних.

Таблиця 2.

Слабкі сторони та рекомендації їх захисту

Слабкі сторони	*Рекомендації*
Використання незахищених Wi-Fi мереж	Забезпечення VPN для всіх пристроїв; навчання співробітників запобігати випадковим та небезпечним підключення в публічних просторах (кафе, бари, ресторани, тощо). Рекомендовано використовувати корпоративні VPN-сервіси, такі як Cisco AnyConnect або OpenVPN, які гарантують шифрування даних
Відсутність шифрування пристроїв	Увімкнення BitLocker або FileVault, впровадження політик MDM для централізованого контролю. Використання MDM-систем (*наприклад*, Microsoft Intune) дозволяє автоматично примусово впровадити шифрування передачі даних пристроїв

Викрадення або втрата пристрою	Автоматичне відключення доступу до ресурсів у разі заволодіння фізичним пристроєм, віддалене очищення критичних даних. Встановлення програм для дистанційного очищення, таких як Prey або Find My Device, допомагає швидко нейтралізувати загрозу несанкціонованого доступу з боку третіх осіб

Висновки. Децентралізоване середовище міжнародної рекламної агенції вимагає комплексного підходу до кібербезпеки та захисту інтелектуальних прав. Використання Zero Trust Architecture, багатофакторної автентифікації, UEBA- та SIEM-систем знижує ризики компрометації даних і забезпечує безпечний доступ до корпоративних ресурсів. Особисті пристрої потребують MDM, шифрування та засобів для віддаленого очищення даних.

Захист інтелектуальної власності на контент і витвори є ключовим для конкурентоспроможності агенції. DRM рішення запобігають несанкціонованому копіюванню, а моніторинг змін у хмарних середовищах і аудит дій користувачів забезпечують контроль. Відділ організації, відподідальний за кібербезпеку має забезпечити реагування на порушення, впроваджуючи технології захисту авторських прав і моніторинг контенту. Такий підхід гарантує як збереження даних, так і захист інтелектуальної власності, що є основою успіху агенції.

Інформаційні джерела

1. Verizon. Data Breach Investigations Report 2023. Verizon Communications, 2023. URL: https://www.verizon.com/business/resources/reports/dbir/

УДК 004.056.5

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАХИЩЕНИХ КАНАЛІВ, ПОБУДОВАНИХ НА ПРОТОКОЛАХ WIREGUARD ТА OPENVPN

Богдан ФІЛІПЧУК
Ростислав ТКАЧУК
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The article provides a comparative analysis of secure channels built on the WireGuard and OpenVPN protocols, with an emphasis on their performance, flexibility, compatibility, and security. WireGuard is characterized by high speed, ease of configuration, and modern cryptographic algorithms, which makes it optimal for mobile devices and simple networks. OpenVPN provides wide versatility, support for legacy systems and complex network architectures, but is inferior to WireGuard in speed and resource consumption. The conclusion emphasizes that the choice between the protocols depends on the context of use: WireGuard is suitable for fast and simple solutions, and*

OpenVPN is suitable for complex corporate environments with high requirements for configuration and compatibility.

Keywords: *WireGuard, OpenVPN, VPN protocol, performance, security, cryptography, compatibility, corporate networks.*

Анотація. *У статті здійснено порівняльний аналіз захищених каналів, побудованих на протоколах WireGuard та OpenVPN, з акцентом на їхню продуктивність, гнучкість, сумісність і безпеку. WireGuard вирізняється високою швидкістю, простотою налаштувань та сучасними криптографічними алгоритмами, що робить його оптимальним для мобільних пристроїв та простих мереж. OpenVPN забезпечує широку універсальність, підтримку застарілих систем і складних мережевих архітектур, але поступається WireGuard у швидкодії та ресурсозатратності. Висновок підкреслює, що вибір між протоколами залежить від контексту використання: WireGuard підходить для швидких і простих рішень, а OpenVPN – для складних корпоративних середовищ із високими вимогами до налаштувань і сумісності.*

Ключові слова: *WireGuard, OpenVPN, VPN-протокол, продуктивність, безпека, криптографія, сумісність, корпоративні мережі.*

У сучасному світі зростає потреба в захищених каналах зв’язку через збільшення кіберзагроз, витоків даних та конфіденційної інформації. Організації та особи прагнуть забезпечити безпечний зв’язок у їхніх онлайн-діях, що підвищує актуальність вивчення сучасних протоколів, таких як WireGuard та OpenVPN.

Метою даної роботи є порівняння протоколів WireGuard і OpenVPN за ключовими характеристиками: безпекою, продуктивністю та зручністю використання. Завдання полягає у вивченні особливостей кожного з протоколів, доходячись до рекомендацій щодо їх використання в різних сценаріях.

WireGuard – це сучасний, високошвидкісний і безпечний VPN-протокол із мінімальною кодовою базою, розроблений для спрощення налаштування та підвищення продуктивності мережі. Його відрізняє мінімалізм і орієнтованість на безпеку, що робить його особливо затребуваним у конфіденційних та продуктивних VPN-системах. Важливою особливістю WireGuard є мінімальна база кодів: він складається лише з кількох тисяч рядків коду, що проводить аудит і перевірку на вразливість у порівнянні з іншими VPN-протоколами, такими як OpenVPN чи IPsec. Це полегшує виявлення та усунення ваших проблем безпеку [1].

WireGuard використовує сучасні криптографічні алгоритми, зокрема ChaCha20 для шифрування, Poly1305 для аутентифікації, Curve25519 для обміну ключами та BLAKE2s для хешування, що забезпечує надійний захист даних і високу продуктивність. Налаштування WireGuard максимально просто й може обмежувати інсталяційні ключі та IP-адресу, що робить його зручним як для адміністраторів, так і для кінцевих корінь.

Протокол забезпечує високу швидкість передачі даних і низьких затримок, працює на рівнях ядра Linux, завдяки чому перевершує продуктивність

багатьох інших VPN-протоколів, особливо на мобільних та вбудованих пристроях. Також WireGuard підтримує роумінг і автоматично відновлює з'єднання при зміні IP-адреси, що особливо зручно для користувачів, які часто змінюють мережу. У протоколі використовується модель ключів без статичної IP-адресації, де обмін ключами побудований на методі криптографічної перевірки ідентифікаторів, що знижує ймовірність витоку даних і ускладнює аналіз трафіку. Завдяки своїй простоті, безпеці та високій продуктивності WireGuard широко використовується в корпоративних і хмарних VPN-мерах [2].

OpenVPN є одним із найпопулярніших та багатофункціональних VPN-протоколів, що забезпечує високу гнучкість у налаштуванні та сумісність із різними мережевими конфігураціями. Використовуючи криптографічні алгоритми, такі як AES для шифрування та SHA для хешування, OpenVPN забезпечує високий рівень захисту даних при їх передачі через незахищені мережі. Завдяки інтеграції з OpenSSL протокол підтримує функції аутентифікації, включно із сертифікатами та двофакторною аутентифікацією, що підвищує надійність підключення [3].

Особливістю OpenVPN є його здатність працювати як на UDP, так і на TCP-портах, що дозволяє ефективно обходити мережеві обмеження та підтримувати стабільність з'єднання в умовах фільтрації трафіку. Додатково, можливість роботи через порт HTTPS забезпечує приховування VPN-трафіку серед звичайного веб-трафіку, що є важливим для обхід блокувань у країнах із суворою цензурою. OpenVPN підтримує як точка-точка, так і клієнт-сервер архітектури, що робить його придатним як для персонального, так і для корпоративного використання [4–6].

Протокол вирізняється підтримкою широкого спектра платформ, включно з Windows, macOS, Linux, Android та iOS, що забезпечує універсальність його використання. Для адміністраторів OpenVPN пропонує розширені можливості управління, такі як налаштування рівнів доступу, обмеження швидкості та дозволів, що робить його ефективним рішенням для корпоративних мереж зі складними політиками безпеки. Поєднання високої гнучкості, надійного шифрування та сумісності робить OpenVPN провідним VPN-протоколом, придатним для застосування у різноманітних мережевих середовищах [7–9].

WireGuard і OpenVPN є провідними VPN-протоколами, але мають різні переваги. WireGuard вирізняється швидкістю, мінімалістичним дизайном і сучасними криптографічними алгоритмами, що робить його ідеальним для мобільних пристроїв та простих конфігурацій. Завдяки мінімальній кодовій базі він забезпечує високий рівень безпеки та простоту використання, але обмежений у гнучкості для складних сценаріїв. OpenVPN, натомість, пропонує широку сумісність, багаті налаштування та підтримку навіть застарілих систем, що робить його незамінним у корпоративних середовищах і мережах із суворими обмеженнями. Проте OpenVPN поступається WireGuard у

швидкості, простоті й продуктивності, але залишається надійним вибором для складних та універсальних VPN-рішень (табл. 1) [10–11].

Таблиця 1.

Порівняння OpenVPN та WireGuard

Характеристика	*WireGuard*	*OpenVPN*
Кодова база	Мінімальна (~4 тис. рядків), легка для аудиту	Велика, складна для перевірки (~сотні тисяч рядків)
Швидкість	Висока, мінімальні затримки завдяки роботі в ядрі Linux	Помірна, вища затримка через роботу в користувацькому просторі
Гнучкість	Мінімалістична, прості налаштування, обмежений функціонал	Висока, підтримка складних конфігурацій і багатих налаштувань
Сумісність	Залежність від сучасних ОС, менше підтримки старих платформ	Універсальна, підтримка навіть застарілих пристроїв
Безпека	Використовує лише сучасні алгоритми, без “старих” опцій	Гнучкість налаштувань може призвести до помилок безпеки
Мобільність	Швидке перепідключення, ідеально для роумінгу	Затримки при перепідключенні через зміну мереж

На основі порівняння WireGuard та OpenVPN можна зробити висновок, що кожен із протоколів має свої переваги і обмеження, що визначають їхню доцільність для конкретних завдань (рис. 1).

Рисунок 1 – Протоколи VPN: WireGuard та OpenVPN

WireGuard демонструє високу продуктивність завдяки мінімалістичній архітектурі, роботі на рівні ядра операційної системи та використанню сучасних криптографічних алгоритмів, що робить його ідеальним вибором для мобільних пристроїв, динамічних середовищ і мережевих сценаріїв із високими вимогами до швидкості та ефективності. Водночас OpenVPN забезпе-

чує широку сумісність і гнучкість, підтримуючи великий спектр платформ, алгоритмів шифрування та розширених налаштувань, що є критично важливим для складних корпоративних середовищ, мереж із застарілими системами та умов, де необхідна максимальна адаптивність. Проте простота та продуктивність WireGuard роблять його менш придатним для складних сценаріїв із численними користувачами чи специфічними вимогами до мережевої архітектури, тоді як OpenVPN може бути менш ефективним у швидкості та ресурсозатратнішим через свою складність.

Висновки. Таким чином, вибір протоколу залежить від контексту використання: WireGuard оптимальний для сучасних і простих конфігурацій, тоді як OpenVPN залишається незамінним у задачах, що вимагають гнучкості, універсальності та підтримки складних інфраструктур. Вибір між WireGuard та OpenVPN слід робити залежно від завдань: обирайте WireGuard для швидких і простих конфігурацій, а OpenVPN – для складних середовищ із високими вимогами до гнучкості та сумісності.

Інформаційні джерела

1. OpenVPN vs WireGuard: який VPN краще? URL: https://hyperhost.ua/info/uk/openvpn-vs-wireguard-yakii-vpn-krashhe (дата звернення: 15.11.2024).

2. Stallings W. (2000). Network Security Essentials: Applications and Standards (pp. 45–60). Prentice Hall.

3. Snader J. C. (2006). VPNs Illustrated: Tunnels, VPNs, and IPsec (pp. 78–102). Addison-Wesley.

4. Donenfeld J. A. (2020). WireGuard: Next-Generation VPN (pp. 15–30). WireGuard.

5. Keijser J. J., & Ali S. (2014). The OpenVPN Cookbook (pp. 34–56). O'Reilly Media.

6. Sanders C., & Smith J. (2013). Applied Network Security Monitoring: Collection, Detection, and Analysis (pp. 120–135). Syngress.

7. Information-resource and cognitive concept of threat's influence identification on technogenic system based on the cause and category diagrams integration. L. Sikora, N Lysa, I. Dronyuk, O. Fedevych, R. Tkachuk, R. Talanchuk. CEUR Workshop Proceedings, pp. 398–416.

8. Military Applications of Data Analytics. New York : Auerbach Publications, 2018. 218 c.

9. Information and laser technologies for data flow selection and their cognitive interpretation in automated control systems. B. V. Durnyak, B. V. Durniak, L. S. Sikora, N. K. Lysa, R. L. Tkachuk, B. I. Yavorsky. Lviv: Ukrainian Academy of Printing.

10. Когнітивні моделі формування стратегій оперативного управління інтегрованими ієрархічними структурами в умовах ризиків і конфліктів: Монографія. Б. В. Дурняк, Л. С. Сікора, М. С. Антоник, Р. Л. Ткачук. Львів: Українська академія друкарства, 2013. – 449 с.

11. Порівняння протоколів VPN. URL: https://www.vpnunlimited.com/ua/help/vpn-protocols/comparison?srsltid=AfmBOooMlsJoDp4YGFAbJc4Q0JkV676mdjOzB3DziB23SqrLfBimjJw7 (дата звернення: 15.11.2024).

УДК 004.838

СУЧАСНІ МЕТОДИ БОРОТЬБИ З АТАКАМИ ТИПУ SQL-ІН'ЄКЦІЙ

Віталій СВІТЛИЧНИЙ
Іван КОВТУН
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *With the increasing popularity of web applications, SQL injection remains one of the most serious cyber threats. This type of attack allows attackers to gain unauthorized access to databases, modify or delete information. The main causes of vulnerabilities are insufficient validation of entered data and the lack of proper security measures. The article reviews modern methods of combating SQL injection, such as input sanitization, parameterized queries, the use of ORM, web application firewalls (WAFs), and database software updates. A comparative analysis of tools for detecting and protecting against SQL injection attacks is presented. The use of comprehensive security measures significantly reduces risks and increases the resilience of information systems in the digital world.*

Keywords: *SQL injection, web applications, cybersecurity, databases, parameterized queries, ORM, WAF, vulnerabilities, protection tools, tool analysis.*

Анотація. *Зі зростанням популярності веб-додатків SQL-ін'єкції залишаються однією з найсерйозніших кіберзагроз. Цей вид атаки дозволяє зловмисникам отримувати несанкціонований доступ до баз даних, модифікувати або видаляти інформацію. Основними причинами вразливостей є недостатня перевірка введених даних та відсутність належних заходів безпеки. У статті розглянуто сучасні методи боротьби з SQL-ін'єкціями, такі як очищення введення, параметризовані запити, застосування ORM, брандмауери веб-додатків (WAF) та оновлення програмного забезпечення баз даних. Представлено порівняльний аналіз інструментів для виявлення та захисту від атак SQL-ін'єкцій. Використання комплексних заходів безпеки сприяє значному зменшенню ризиків і підвищує стійкість інформаційних систем у цифровому світі.*

Ключові слова: *SQL-ін'єкція, веб-додатки, кібербезпека, бази даних, параметризовані запити, ORM, WAF, вразливості, засоби захисту, аналіз інструментів.*

Зі зростанням кількості веб-додатків і залежності сучасного світу від цифрових даних атаки типу SQL-ін'єкцій залишаються однією з найсерйозніших загроз у сфері кібербезпеки. Цей вид атаки дозволяє зловмисникам отримувати несанкціонований доступ до баз даних, маніпулювати інформацією та навіть видаляти важливі дані. Незважаючи на відомість проблеми, багато організацій досі стикаються з труднощами у забезпеченні належного рівня захисту своїх систем. Сучасні методи боротьби з SQL-ін'єкціями спрямовані на впровадження комплексних підходів, які поєднують вдосконалені технології захисту, кращі практики програмування та ефективні методи виявлення вразливостей.

SQL-ін'єкція є видом атаки на веб-додатки, при якому зловмисники експлуатують вразливості в обробці введених користувачем даних для впрова-

дження та виконання шкідливого SQL-коду на сервері бази даних. Ця атака стає можливою через недостатню перевірку та фільтрацію даних, що дозволяє змінювати SQL-запити через веб-інтерфейс і отримувати несанкціонований доступ до інформації. Витоки SQL-ін'єкцій сягають кінця 1990-х років, коли веб-додатки стали більш популярними для доступу до баз даних. З розповсюдженням технологій, таких як PHP і ASP, стало очевидно, що багато додатків не забезпечували належної перевірки введених даних, що створило можливості для зловмисників, які почали активно використовувати ці вразливості [1].

Хоча атаки SQL-ін'єкцій можуть бути дуже небезпечними, їх можна запобігти за допомогою належних заходів безпеки.

Очищення введення. Один з ефективних способів протидії атакам полягає в очищенні введених даних перед їх використанням у SQL-запитах. Це включає видалення або екранування спеціальних символів, таких як одинарні та подвійні лапки, які можуть бути використані для впровадження шкідливого коду [4].

Параметризовані запити. Цей підхід дозволяє відокремити SQL-код від введених даних користувача, ускладнюючи їх використання для атак. Завдяки параметризованим запитам дані користувача обробляються виключно як значення, а не як код [3].

Застосування ORM (Object-Relational Mapping). Використання фреймворків ORM допомагає зменшити ризик SQL-ін'єкцій, оскільки вони забезпечують абстрагування бази даних і автоматичне створення безпечних SQL-запитів. Важливо переконатися, що фреймворк безпечно обробляє введення даних [4].

Брандмауери веб-додатків (WAF). WAF є потужним інструментом для захисту веб-додатків від SQL-ін'єкцій та інших загроз. Вони перевіряють вхідний трафік на наявність зловмисних даних, створюючи додатковий рівень захисту [3].

Оновлення програмного забезпечення баз даних. Постійне оновлення систем керування базами даних допомагає захиститися від відомих вразливостей, які можуть бути використані для атак SQL-ін'єкцій. Регулярне оновлення та виправлення усувають недоліки безпеки та підвищують стійкість системи (табл. 1) [3].

Таблиця 1.

Аналіз сервісів та інструментів для боротьби з атаками типу SQL-ін'єкцій

Характеристика	*SQLMap*	*Acunetix*	*OWASP ZAP*	*Burp Suite*
Платні функції	ні	так	так (платно / безкоштовно)	так
Автоматичне виявлення SQL-ін'єкцій	так	так	так	так
Захист від SQL-ін'єкцій у реальному часі	ні	так	ні	ні
Інтеграція з системами CI/CD	ні	так	так	так

Аналіз вразливостей	так	так	так	так
Підтримка складних конфігурацій запитів	так	так	ні	так
Кількість доступних баз даних для тестування	6+	10+	5+	8+

Висновки. У підсумку, сучасні методи боротьби з атаками типу SQL-ін'єкцій є важливою складовою забезпечення кібербезпеки. Використання підходів, таких як параметризовані запити, оновлення та виправлення програмного забезпечення бази даних та використання ORM (Object-Relational Mapping), значно підвищує стійкість веб-додатків до потенційних загроз. Інтеграція новітніх технологій захисту, регулярний аудит безпеки та навчання розробників у сфері безпечного кодування сприяють створенню ефективного захисту від атак SQL-ін'єкцій. Комплексне застосування цих заходів дозволяє мінімізувати ризики та забезпечити надійний захист інформаційних систем, що є критично важливим у сучасному цифровому світі.

Інформаційні джерела

1. SQL ін'єкції та захист від них. URL: https://foxminded.ua/sql-iniektsii/ (дата звернення 17.11.2024).
2. SQL Injection Attack: How It Works, Examples and Prevention. URL: https://brightsec.com/blog/sql-injection-attack/ (дата звернення 17.11.2024).
3. How to Prevent SQL Injection Attacks: 6 Proven Methods. URL: https://www.strongdm.com/blog/how-to-prevent-sql-injection-attacks (дата звернення 17.11.2024).
4. SQL ін'єкції та захист від них. URL: https://foxminded.ua/sql-iniektsii/ (дата звернення 17.11.2024).

УДК 004.451.64

ОПЕРАТИВНЕ УПРАВЛІННЯ В ІЄРАРХІЧНО-СТРУКТУРОВАНИХ СИСТЕМАХ ТА ВИБІР МОДЕЛЕЙ СТРАТЕГІЙ ЦІЛЕОРІЄНТОВАНИХ ДІЙ В УМОВАХ ЗАГРОЗ

Володимир КУГОТ
Володимир САБАТ
Інститут поліграфії та медійних технологій Національного університету "Львівська Політехніка", м. Львів, Україна.

Abstract. *Methods and problems of planning and management in hierarchically structured systems are considered. The main integration procedures for assessing situations in crisis conditions, integration of the operator into the structure and processes of management in hierarchical systems, coordination of his actions in them are highlighted. The classification of information data in decision-making procedures is given and the information security formed on the normative-algorithmic model of the management object is proposed.*

Keywords: *management, decision-making, behavioral strategy, management system.*

Анотація. *Розглянуто способи та проблеми планування і управління в ієрархічно-структурованих системах. Виокремленні основні інтеграційні процедури оцінки ситуацій у кризових умовах, інтеграцію оператора в структуру і процеси управління в ієрархічних системах, координацію його дій у них. Надано класифікацію даних інформації в процедурах прийняття рішень і запропоновано інформаційне забезпеченняке формується на нормативно-алгоритмічній моделі об'єкта управління.*

Ключові слова: керування, прийняття рішень, стратегія поведінки, система управління.

Оперативне управління командами, в умовах нормальних і надзвичайних ситуацій в технологічних виробничих системах і господарських комплексах, при природних катастрофах, ґрунтується на оперативному плануванні і супервізорному синхронному керуванні всіма компонентами системи та людським колективом, а також неорганізованими масами людей які опинились в загрозливій ситуації [1].

Найбільш важливим елементом керування такими інтегрованими об'єктами є забезпечення тактичного рівня безпеки для прийняття як операційних рішень, так і на циклі термінального часу їх функціонування. Тому актуальною проблемою системного стратегічного управління інтегрованими структурами [ІС] є побудова моделей і алгоритмів інтегрованого керування та планування дій для оперативного розв'язання цільових, поточних і кризових ситуацій.

Інтеграція планування і управління в ієрархічно-структурованих системах ґрунтується на побудові концептуальних моделей компонент і всієї структури, які відповідно будуть основою аналізу поточної динаміки і синтезу цілеорієнтованих стратегій поведінки як оператора, так і автоматизованих управляючих комплексів [1–3].

Формалізований опис системи повинен будуватись з використанням однотипного математичного апарату (графи, дослідження операцій, теорія ігор та прийняття рішень), а для його стикування необхідно застосовувати пов'язуючі оптимізаційні алгоритми.

Для оперативного управління інтегрованими автоматизованими системами управління [ІАСУ] ефективною є трьохрівнева система планування і управління:

– ситуаційний рівень;

– оперативний рівень прийняття рішень;

– календарний рівень планування функціонування системи.

На кожному рівні виділені цикли і фази елементів планування і реалізації запланованих дій, з використанням інформаційної бази в діалоговому режимі. Для забезпечення процедур прийняття рішень в умовах невизначеності при цільовому плануванні використовується принцип послідовного розкриття невизначеностей і моделі ігрових ситуацій для імітації сценаріїв поведінки.

Класичні результати одержані у вигляді комплексів математичних моделей і алгоритмів багатокритеріального лінійного програмування, з врахуванням ресурсів та обмежень на них. Процедура багатокритеріального управління узгоджує функціонування всіх рівнів системи.

Функціональна процедура ранжування локальних критеріїв оптимізації використовує методи шкал та методи прискореної сходимості в алгоритмах оптимального прийняття рішень, що є основою чіткої формалізації процедури прийняття управлінських рішень у виробничих умовах [1].

Нижчі рівні ІАСУ можна описати на основі модифікації під об'єкт динамічної імітаційної моделі як в неперервному так і дискретному режимах, або у вигляді кусочно-лінійних автоматів [5].

На рівні операційного управління [1, 6] використовують багатокрокові інтеграційні процедури оцінки ситуацій (динамічне програмування і теорія статистик), при цьому:

– розкриваються процеси планування і прийняття рішень на основі вибору алгоритмів дій;

– розгортаються моделі дій в часі і просторі згідно цільових планів і стратегій управління;

– коректуються процеси управління на основі отриманої оперативної інформації;

– виявляється і оцінюється множина значимих факторів впливу і загроз.

При цьому важливою проблемою залишається інтеграція оператора в структуру ІАСУ і в процеси управління, координації в них. Для розв'язку цієї проблеми обґрунтовано два підходи:

– імітаційне моделювання функціонування ІАСУ з врахуванням ймовірних ситуацій збою режимів, для яких введені стратегії оптимізації і адаптації структури;

– динамічне моделювання ІАСУ основане на цифровому представленні моделей структури і динаміки (графи, сигнали, структуру, потоки), які є основою створення модульних моделей високого рівня.

Такі модулі є логічно-деталізованими моделями [1, 6], проблемно-орієнтованими на розв'язання комплексів задач: аналізу динаміки матеріальних та інформаційних потоків, інтегрованого управління і планування дій, диспетчерського оперативного управління.

Ефективність управління технологічною системою з розподіленою енергоактивною структурою залежить від послідовності приймаючих рішень в динаміці термінального часу. Для прийняття рішень необхідна інформація про оперативну ситуацію в реальному часі, прогноз ходу процесу в системі, дані про минулу поведінку (тенденції).

Оперативність прийняття рішень системою ґрунтується на використанні достатньої і необхідної науково-коректної інформації як від об'єкта про

ситуацію в реальному часі, так і від інтегрованої бази даних і знань. Ця інформація поділяється на [3–5]:

– поточну інформацію, що отримується автоматично;

– інформацію, сформовану оператором на основі аналізу потоків даних;

– попередню інформацію з бази знань і даних;

– інформацію закладену конструктором на діаграмах, мнемосхемах та в документації;

– інформацію опрацьовану та заархівовану оператором, що вимагає еластичності адаптивних структур опрацювання сигналів та даних, їх алгоритмічного і програмного забезпечення.

Відповідно до вимог процедур прийняття рішень інформація в потоках даних класифікується таким чином [1, 4]:

– інформація про структуру і характеристики компонент об'єкта управління (ОУ)-(графи зв'язків, канали, давачі, потоки);

– інформація про динаміку ОУ і АСУ;

– інформація про зовнішнє середовище, його параметри і характеристики;

– інформація про збурення і загрози;

– інформація про цілі функціонування ОУ і АСУ, критерії якості та обмеження;

– інформація про допустимі та оптимальні стратегії тактики планування дій і управління ними в умовах невизначеності критеріїв ефективності та відомостей про дію загроз і збурень.

Тобто при прийнятті цільових рішень виникають ситуації при яких немає достатньої інформації про поведінку системи в цілому. Виникають непрогнозовані стохастичні загрози, в систему управління вклинюються активні елементи (особи) з регламентованою свободою дій та поведінки при прийнятті нестандартних рішень та виконання дій.

У таких випадках класичні теорії ймовірності, ігор, оптимального управління, ідентифікації і адаптації не забезпечують відповідну логіку планування дій. Тому для вищевказаних випадків управління в ІАСУ важливо сформувати відповідне інформаційне забезпечення, в яке входять [1–3]:

– сукупність відомостей в масивах і потоках даних, документах, сигналах;

– методи організації, структурування та збереження масивів даних;

– оперативні дані: адміністративні, економічні, технологічні, нормативні;

– відомості про функціональні зв'язки елементів і блоків системи;

– логіко-математичні елементи процедур прийнятті рішень (логіка рішень і дій);

– моперативне відображення інформації про стан системи і хід процесів;

– методи зберігання управляючих програм (моделі стратегій і тактик цільових дій алгоритмів).

Висновки. Цільова картина системи формується на нормативно-алгоритмічній моделі [НАМ] як сукупність інформаційної моделі об'єкта

керування і алгоритмів опрацювання даних і прийняття управлінських рішень узгоджених з організаційною структурою.

Інформаційні джерела

1. Резниченко С. С., Подольский М. П., Шихман А. А. Экономико-математические методы и моделирование в планировании и управлении горным производством. К.: Наука, 1991. 429 с.

2. Лигум Ю. С. Автоматизированные системы управления технологическими процессами пассажирского автомобильного транспорта. К.: Техніка, 1989. 239 с.

3. Сікора Л. С. Системологія прийняття рішень на управління в складних технологічних структурах. – Львів: Каменяр, 1998. 453 с.

4. Литвинов В. В., Марянович Т. П. Методы построения имитационных систем. К. Наукова думка, 1991. 120 с.

5. Системы автоматизированного проектирования и диспетчеризация производственных процессрв / под ред. Павлова А. А. К.: Техніка, 1990. 198 с.

6. Информационные технологии в испытаниях сложных объектов: методы и средства / ред. Скурихин В. И. К.: Наукова Думка, 1990. 320 с.

УДК 004.056.5:340

ЗАХИСТ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ: ПРАКТИКИ ТА ПЕРСПЕКТИВИ В УКРАЇНІ

Ілля ГОНЧАРУК
Олександр МАНЖАЙ
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article compares the legislation and strategic approaches of Ukraine and the United States in the field of cybersecurity. Key differences in the development of the regulatory framework, financing, protection of critical infrastructure, training of personnel, and international cooperation are analyzed. It is determined that the United States has significant experience and a developed infrastructure, while Ukraine is actively developing its own cyber defense system, focusing on critical infrastructure and harmonizing legislation with European standards. The importance of global cooperation for creating a secure cyberspace is emphasized.*

Keywords: *cybersecurity, legislation, critical infrastructure, cyber defense strategy, Ukraine, United States, international cooperation, cybersecurity personnel.*

Анотація. *У статті порівнюється законодавство та стратегічні підходи України й США у сфері кібербезпеки. Проаналізовано ключові відмінності в розвитку нормативної бази, фінансуванні, захисті критичної інфраструктури, підготовці кадрів та міжнародній співпраці. Визначено, що США мають значний досвід і розвинену інфраструктуру, тоді як Україна активно розвиває власну систему кіберза-*

хисту, зосереджуючись на критичній інфраструктурі та гармонізації законодавства з європейськими стандартами. Підкреслено важливість глобальної співпраці для створення безпечного кіберпростору.

Ключові слова: *кібербезпека, законодавство, критична інфраструктура, стратегія кіберзахисту, Україна, США, міжнародна співпраця, кадри з кібербезпеки.*

Законодавство України у сфері кібербезпеки почало формуватися активно після 2017 року, коли було ухвалено Закон "Про основні засади забезпечення кібербезпеки". У США розвиток цієї сфери почався значно раніше, у першій половині XX століття, з ухвалення законів про захист комп'ютерних систем, *наприклад*, Закон "Про комп'ютерну безпеку" та Закон "Про удосконалення інформаційної безпеки". Це дало США перевагу в тривалості адаптації законодавства до сучасних кіберзагроз. Україна розробила стратегію кібербезпеки на 2016–2020 роки та планує оновлення на 2020–2025 роки. США мають більш детальну та розгалужену стратегію, яка включає документи, такі як "Національна стратегія захисту кіберпростору" (2003), "Огляд з кібербезпеки" (2009) та "Стратегія кібербезпеки" (2011). Американські стратегії містять чіткі заходи та цілі, зокрема створення федеральної мережі для боротьби з кібератаками та розвиток кібер контррозвідки.

В Україні сфера кібербезпеки регулюється єдиним всеосяжним законом, який надає повноваження основним державним органам, таким як СБУ та ДССЗЗІ. У США законодавча база включає десятки федеральних та штатних законів, що регулюють різні аспекти, від кіберзлочинності Закон "Про комп'ютерне шахрайство та зловживання" до конфіденційності даних Закон "Про охорону персональних даних". Така деталізація дозволяє враховувати різні типи загроз і суб'єктів.

В Україні основними виконавцями у сфері кібербезпеки є СБУ та ДССЗЗІ. У США кібербезпека координується Департаментом внутрішньої безпеки (DHS), який співпрацює з багатьма федеральними установами, зокрема ФБР та Секретною службою, вони також мають централізовану мережу центрів оперативного реагування на кібератаки, що забезпечує швидкість і ефективність реагування.

Бюджет США на кібербезпеку значно перевищує витрати України. У 2016 році США виділили $14 млрд на кібербезпеку, тоді як фінансування України є набагато скромнішим через економічні обмеження, це впливає на можливості реалізації стратегій і розвитку інфраструктури.

В Україні основний акцент робиться на критичній інфраструктурі (КІ), однак механізми її захисту лише формуються. У США захист КІ є ключовим пріоритетом ще з початку 2000-х років, зокрема після ухвалення "Ініціативи зі всеосяжної національної кібербезпеки".

Обидві країни визнають важливість підготовки кадрів. В Україні ця сфера лише розвивається, тоді як у США давно впроваджені освітні програми з кібербезпеки на державному рівні, а також створено кібер підрозділи у

провідних університетах. Україна активно співпрацює з ЄС у сфері гармонізації законодавства з Директивою NIS. США зосереджені на міжнародних ініціативах і укладенні угод з кібербезпеки, які часто мають глобальне значення, *наприклад*, у рамках НАТО чи G7.

Висновки. В Україні довіра до систем кіберзахисту держави обмежена через слабку інформованість і технічні недоліки. У США цифрова грамотність і страхування кібер ризиків сприяють підвищенню довіри громадян до уряду, хоча проблема кіберзлочинності залишається актуальною. Хоча Україна досягає значного прогресу в розвитку кібербезпеки, США мають переваги завдяки тривалому досвіду, розвиненій інфраструктурі та значним фінансовим ресурсам. Обидві країни об'єднує прагнення створити безпечний кіберпростір, але підходи до реалізації цієї мети суттєво різняться.

Інформаційні джерела

1. Порівняльний аналіз регулювання кібербезпеки 5G в Україні на Європейських країнах: Німеччині, Швеції, Фінляндії та країнах Балтії. URL: https://vaibit.org.ua/comparative-analysis-of-5g-cybersecurity-regulation/ (дата звернення: 20.11.2024).

2. Секрет успіху США у сфері інформаційної безпеки. URL: https://relint.vnu.edu.ua/index.php/relint/article/view/28/15 (дата звернення: 19.11.2024).

3. Правова база української кібербезпеки. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf (дата звернення: 18.11.2024).

4. Поняття та зміст національної системи кібербезпеки. URL: https://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/ (дата звернення: 19.11.2024).

УДК 343.9:004.056

ОКРЕМІ АСПЕКТИ ПРОТИДІЇ КІБЕРШАХРАЙСТВУ

Максим РУДЕНКО
Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article examines the problem of cyber fraud as a key challenge for law enforcement agencies in the modern digital environment. The main forms of fraud, anonymization tools and the international scale of crimes that complicate investigations are analyzed. Particular attention is paid to the use of modern technologies, such as artificial intelligence and machine learning, to detect fraud schemes and analyze data. The importance of increasing digital literacy among the population, developing a legal framework and international cooperation as necessary conditions for effectively combating cybercrime is emphasized.*

Keywords: *cyberfraud, law enforcement agencies, artificial intelligence, digital literacy, anonymization, international cooperation, cybersecurity, prevention.*

Анотація. *Стаття досліджує проблему кібершахрайства як ключового виклику для правоохоронних органів у сучасному цифровому середовищі. Аналізуються основні форми шахрайства, інструменти анонімізації та міжнародний масштаб злочинів, що ускладнюють розслідування. Особливу увагу приділено використанню сучасних технологій, таких як штучний інтелект та машинне навчання, для виявлення схем шахрайства та аналізу даних. Підкреслюється важливість підвищення цифрової грамотності серед населення, розвитку правової бази та міжнародної співпраці як необхідних умов для ефективної боротьби з кіберзлочинністю.*

Ключові слова: *кібершахрайство, правоохоронні органи, штучний інтелект, цифрова грамотність, анонімізація, міжнародна співпраця, кібербезпека, профілактика.*

Боротьба з кібершахрайством є одним з ключових завдань сучасних правоохоронних органів. З бурхливим розвитком цифрових технологій шахраї отримують нові інструменти для реалізації своїх злочинних намірів. Від фішингових атак і крадіжки персональних даних до фінансового шахрайства і використання криптовалют для приховування коштів, кібершахрайство приймає все більш витончені форми. Це створює серйозні проблеми для правоохоронних органів, які змушені адаптуватися до нових умов і розробляти інноваційні способи боротьби з цим явищем.

Одна з основних проблем полягає у швидкому розвитку технологій, які злочинці використовують для маскування своїх дій. Інструменти для анонімізації, такі як VPN, даркнет або криптовалюти, значно ускладнюють ідентифікацію злочинців і відстеження їхньої діяльності. Крім того, характер кібершахрайства часто має міжнародний масштаб, що потребує тісної співпраці між правоохоронними органами різних країн. Міжнародні юридичні бар'єри, відсутність уніфікованих стандартів у боротьбі з кіберзлочинами та обмежений доступ до даних ще більше ускладнюють ефективне розслідування [1].

Не менш важливою проблемою є недостатній рівень цифрової грамотності серед населення. Жертви кібершахрайства часто стають легкою мішенню через брак базових знань у сфері кібербезпеки. Це вимагає посиленої профілактичної роботи правоохоронних органів у вигляді інформаційних кампаній та навчальних заходів, спрямованих на підвищення обізнаності громадян про основні види шахрайства та способи їх уникнення.

Водночас для ефективної боротьби з кібер-шахрайством необхідні сучасні технологічні рішення. Використання штучного інтелекту та машинного навчання може значно спростити аналіз великих обсягів даних, передбачити шахрайські схеми та автоматизувати багато етапів дослідження. Крім того, важливо навчати співробітників правоохоронних органів. Вони навчені новим способам роботи з цифровими доказами і знайомі з новітніми технологіями виявлення і розслідування кіберзлочинів.

Для забезпечення довгострокової ефективності необхідно розробити правову базу в області кібербезпеки і привести її у відповідність з міжнародними стандартами. Співпраця, обмін досвідом і технологіями між країнами є ключовими для декомунізації в боротьбі з транснаціональною кіберзлочинністю.

Боротьба з кібер-шахрайством-непросте завдання, але завдяки системному підходу, інноваційним технологіям та добре скоординованій роботі правоохоронних органів рівень злочинності в цифровому просторі може бути значно знижений. Це не тільки захищає громадян від шахрайства, а й сприяє підвищенню довіри до правоохоронних органів і зміцненню інформаційної безпеки в суспільстві в цілому.

Не менш важливим є те, що боротьба з кібер-шахрайством є ключовою проблемою для правоохоронних органів у сучасному цифровому світі. Злочинці активно використовують технологічні інновації для приховування своєї діяльності, і правоохоронним органам необхідно постійно вдосконалювати свої підходи та інструменти боротьби з кіберзлочинністю. Інтеграція штучного інтелекту, розвиток міжнародного співробітництва та професійний розвиток є необхідними умовами для ефективного реагування на ці загрози.

Висновки. Отже важливим аспектом є профілактика, зокрема інформування громадян та підвищення їх цифрової грамотності. Лише комплексний підхід, що поєднує технологічні, правові та освітні аспекти, дозволить забезпечити безпеку у цифровому просторі та зменшити вплив кібершахрайства на суспільство. Успішна реалізація цих заходів сприятиме не лише захисту громадян, але й зміцненню довіри до правоохоронної системи.

Інформаційні джерела

1. Ablamskyi S., Romaniuk V., Ablamska V. Cybercrime and the use of digital technologies: modern challenges to the law enforcement system. Bulletin of Luhansk Scientific-Educational Institute named after E. O. Didenko. 2024. № 1, pp. 254–266. URL: https://doi.org/10.33766/2786-9156.105.254-266 (дата звернення: 20.11.2024).

УДК 004.056.53

АНАЛІЗ ВРАЗЛИВОСТЕЙ В ПОПУЛЯРНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ ТА ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ

Владислав НЕЧИПОРУК
Василь ЛУЧИК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article examines the main vulnerabilities of operating systems, which are key targets of attacks in the modern digital environment. Types of vulnerabilities are analyzed, including code errors, incorrect system settings, lack of updates, and zero-day exploits. Examples of well-known vulnerabilities, such as EternalBlue (Windows) and Dirty COW (Linux), which had global consequences for the security of networks and organizations, are given. The need for a comprehensive approach to vulnerability management is emphasized, including regular system updates, threat monitoring, and user training.*

Keywords: *operating system vulnerabilities, cybersecurity, zero-day exploits, EternalBlue, Dirty COW, system updates, vulnerability management, malware.*

Анотація. *У статті розглядаються основні вразливості операційних систем, які є ключовими об'єктами атак у сучасному цифровому середовищі. Аналізуються типи вразливостей, зокрема помилки в коді, неправильні налаштування системи, відсутність оновлень та експлойти нульового дня. Наведено приклади відомих вразливостей, таких як EternalBlue (Windows) та Dirty COW (Linux), що мали глобальні наслідки для безпеки мереж та організацій. Підкреслюється необхідність комплексного підходу до управління вразливостями, включаючи регулярне оновлення систем, моніторинг загроз і навчання користувачів.*

Ключові слова: *вразливості операційних систем, кібербезпека, експлойти нульового дня, EternalBlue, Dirty COW, оновлення систем, управління вразливостями, шкідливе програмне забезпечення.*

Сучасний цифровий світ неможливий без операційних систем і програмного забезпечення, які забезпечують функціонування як персональних пристроїв, так і корпоративних мереж. Проте із розвитком технологій зростає кількість і складність кіберзагроз, які використовують вразливості в цих системах. Виявлення, аналіз та усунення таких вразливостей є критично важливими для забезпечення кібербезпеки та захисту даних користувачів і організацій.

Вразливості операційних систем (ОС) є однією з основних причин, що створюють загрози інформаційній безпеці в сучасних мережах. Вони включають слабкі місця в архітектурі, налаштуваннях або програмному забезпеченні ОС, які зловмисники можуть використати для отримання несанкціонованого доступу, впливу на роботу системи або крадіжки даних. Вразливості класифікуються за типами, такими як помилки в коді, слабкі налаштування безпеки, невиправлені патчі та відкриті мережеві порти, що робить операційні системи ключовим об'єктом атак для кіберзлочинців. Одним із найпоширеніших видів вразливостей є помилки в коді операційних систем. Ці помилки можуть виникати через недосконалості в розробці програмного забезпечення або недостатнє тестування, що призводить до появи критичних багів.

Наприклад, експлойти, що використовують помилки в управлінні пам'яттю (таким як переповнення буфера), дозволяють зловмисникам виконувати шкідливий код з привілеями адміністратора. Такі вразливості є основними мішенями для кібератак і потребують регулярного оновлення системи для їх усунення. Ще однією значною категорією вразливостей є неправильні налаштування системи. Вони виникають, коли ОС або програмне забезпечення працюють із відкритими портами або стандартними обліковими записами без змінених паролів, що полегшує доступ зловмисників. Крім того, слабкі політики доступу до файлів і неправильна конфігурація системи захисту дозволяють використовувати системи для поширення шкідливого програмного забезпечення або атак на інші частини мережі. Окрім цього,

вразливості, пов'язані з відсутністю оновлень, залишають системи незахищеними проти вже відомих атак.

Бази даних загальних вразливостей (CVE) регулярно оновлюються новими даними про потенційні загрози, і ОС, які не отримують вчасно оновлень, стають легкою мішенню для експлуатації. Це особливо небезпечно в середовищах, де використовуються застарілі версії програмного забезпечення або системи, для яких уже не надається технічна підтримка. Виявлення та усунення цих вразливостей є критично важливим елементом кібербезпеки. Процес управління вразливостями, що включає регулярне сканування, пріоритетизацію ризиків і застосування виправлень, є стандартом для забезпечення безпеки ОС. Безперервна робота в цьому напрямі дозволяє мінімізувати можливості зловмисників для експлуатації вразливостей та знижує ризик втрати даних або пошкодження систем.

Операційні системи, такі як Windows, macOS та Linux, схильні до різних типів вразливостей, які можуть стати основою для кібератак. Одним із найсерйозніших викликів є експлойти нульового дня – невідомі раніше слабкі місця в системі, які використовуються зловмисниками до випуску виробником оновлень безпеки. Такі експлойти особливо небезпечні, оскільки до моменту їх виявлення система лишається абсолютно незахищеною. *Наприклад*, популярність Windows і її широке використання в корпоративному середовищі робить її частою мішенню для експлойтів нульового дня, особливо в компонентах, пов'язаних із роботою в мережі або управлінням привілеями.

Ще однією розповсюдженою вразливістю є помилки в ядрах ОС, які можуть призводити до серйозних порушень безпеки. Ядро операційної системи – це її основна частина, що керує доступом до ресурсів і виконує критичні операції. Якщо зловмисники отримують доступ до вразливості ядра, вони можуть запускати шкідливий код із найвищими привілеями, що дозволяє повний контроль над системою.

Наприклад, Linux, хоч і вважається однією з найзахищеніших систем, не застрахована від таких помилок, оскільки її відкритий код є доступним для вивчення не лише розробникам, але й хакерам. Проблеми з правами доступу також є важливим аспектом вразливостей сучасних операційних систем. Неправильно налаштовані права доступу до файлів, мережевих ресурсів або привілейованих функцій можуть дати змогу зловмисникам розширити свої права в системі, отримати доступ до конфіденційної інформації або змінити налаштування безпеки. Це особливо актуально для macOS, яка, хоча й відома своєю захищеністю, іноді страждає від неправильно реалізованих обмежень доступу до ключових функцій або файлів.

EternalBlue – це одна з найвідоміших вразливостей операційної системи Windows, ідентифікована під кодом CVE-2017-0144. Вона використовує недоліки реалізації протоколу Server Message Block (SMB) версії 1, що дозволяють зловмиснику надсилати спеціально створені пакети для виконання довільного коду на віддалених системах. Ця вразливість залишалася відкри-

тою понад 16 років і охоплювала системи від Windows XP до Windows Server 2016. Вона стала відомою після витоку хакерської групи The Shadow Brokers у квітні 2017 року, яка оприлюднила дані, ймовірно викрадені з Агентства національної безпеки США. EternalBlue стала основою для таких атак, як поширення вірусу-шифрувальника WannaCry у травні 2017 року, який вразив десятки тисяч комп'ютерів по всьому світу.

Хоч Microsoft випустила оновлення безпеки MS17-010, відсутність регулярного оновлення систем зробила багато мереж уразливими. EternalBlue також мала серйозні наслідки для України, особливо під час атаки вірусу Petya у червні 2017 року. Зловмисники використали експлойт для поширення шкідливого ПЗ через заражений сервіс оновлення бухгалтерської програми M.E.Doc. Цей вірус паралізував роботу численних банків, державних установ і енергетичних компаній. EternalBlue показала критичну важливість своєчасного оновлення систем, особливо для організацій, які залежать від мережевої інфраструктури. Попри те, що Microsoft припинила підтримку деяких старих версій Windows, через масштаби атаки, були випущені спеціальні патчі навіть для застарілих систем. Dirty COW (CVE-2016-5195) є прикладом серйозної вразливості в ядрах Linux, виявленої у 2016 році. Вона існувала понад дев'ять років і була пов'язана з помилкою у функції копіювання даних між процесами (Copy-On-Write). Зловмисники могли скористатися цією вразливістю для підвищення своїх привілеїв у системі, отримуючи доступ до об'єктів із правами суперкористувача.

Висновки. Ефективна боротьба з вразливостями в операційних системах та програмному забезпеченні вимагає комплексного підходу, який включає не лише розробку безпечного коду, але й постійний моніторинг, тестування та швидке реагування на загрози. Організації повинні інвестувати у навчання співробітників з питань кібербезпеки, а також впроваджувати сучасні технології для захисту даних. Водночас, користувачі також мають брати участь у підвищенні власної цифрової грамотності, дотримуючись базових принципів безпеки, таких як регулярне оновлення програмного забезпечення та використання складних паролів. Аналіз вразливостей дозволяє знизити ризики кібератак і сприяє створенню більш безпечного цифрового середовища.

Інформаційні джерела

1. Що таке вразливості в контексті обробки даних: управління вразливостями. URL: https://bsoprivacygroup.com/shcho-take-vrazlyvosti-v-konteksti-obrobky-danykh-upravlinnia-vrazlyvostiamy/ (дата звернення: 16.11.2024).

2. Методи та засоби боротьби з вразливостями комп'ютерних мереж. URL: https://openarchive.nure.ua/server/api/core/bitstreams/5fc436e5-ac7f-4142-8cc4-415abe3fee4d/content (дата звернення: 17.11.2024).

3. Чим небезпечно використовувати Windows на комп'ютері або ноутбуці. URL: https://itechua.com/articles/234081 (дата звернення: 16.11.2024).

4. EternalBlue. URL: https://uk.wikipedia.org/wiki/EternalBlue (дата звернення: 17.11.2024).

УДК: 328.184: 355.404

ЗАХИСТ ВІД ФІШИНГУ ТА РИЗИКИ ВІДКРИТИХ ДЖЕРЕЛ

Богдан ДМИТРУК
Наталія СТЕПАНЧУК
Назарій БУРАК

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The paper explores the main aspects of Internet security, in particular, threats associated with phishing attacks and the use of open source information (OSINT). The possibilities of searching for information by phone number and locating by photos are considered. Recommendations for protecting personal data and preventing fraudulent activities are given.*

Keywords: *Internet security, phishing, personal data protection, OSINT, GeoOSINT.*

Анотація. *У роботі досліджено основні аспекти безпеки в інтернеті, зокрема, загрози, пов'язані з фішинговими атаками та використанням інформації з відкритих джерел (OSINT). Розглянуто можливості пошуку інформації за номером телефону та визначення місця за фотографіями. рекомендації щодо захисту особистих даних і запобігання шахрайським діям.*

Ключові слова: *безпека в інтернеті, фішинг, OSINT, GeoOSINT.*

З розвитком цифрових технологій питання безпеки в інтернеті набувають особливого значення. Однією з найбільших загроз залишається *фішинг* – метод шахрайства, спрямований на викрадення персональних даних користувачів. Така діяльність може призводити до фінансових втрат, втрати конфіденційності та інших ризиків.

Для зменшення ймовірності стати жертвою фішингу варто дотримуватися наступних порад:

ПеревіркаURL-адрес. Завжди ретельно перевіряйте URL-адреси перед переходом за посиланнями. Справжня адреса має виглядати, наприклад, так: https://drive.google.com/drive/.... Якщо ж посилання містить підозрілий або незнайомий домен, як-от security-org.drive.com, варто бути обережними. Зловмисники часто використовують подібні домени або сервіси скорочення URL (*наприклад*, tinyurl), щоб приховати справжнє посилання. При наведенні курсора на кнопку посилання слід перевірити субдомен – він має збігатися з офіційним сайтом, а не містити підозрілих назв.

Підозрілі електронні адреси. Шахраї часто маскуються під представників відомих компаній і надсилають листи з адрес, що можуть виглядати схожими на офіційні. Наприклад, лист від support@googl3.com (де замінено літеру "е" на цифру "3") є підозрілим, імовірно, фішинговим. Варто бути особливо обережними, якщо лист містить прохання негайно надати конфіденційну інформацію.

Наголос на терміновості. Шахраї часто використовують тактику наголошення на терміновості, щоб спонукати вас до поспішних дій. Наприклад, вони можуть зазначити, що ваш рахунок буде заблоковано, якщо ви негайно не підтвердите свої дані. У таких випадках не переходьте за посиланням із листа, а натомість зайдіть на сайт компанії вручну або зв'яжіться з офіційною службою підтримки.

Перевірка реквізитів. Якщо отримали повідомлення з проханням переказати кошти чи надати особисту інформацію, завжди перевіряйте офіційні реквізити компанії. Наприклад, номер телефону можна перевірити на офіційному сайті, перш ніж здійснювати будь-які дії.

Захист двофакторною аутентифікацією. Ніколи не повідомляйте код двофакторної аутентифікації (2FA) за межами процедури входу, яку ви самі ініціювали. Наприклад, якщо ви отримали SMS з кодом, не передавайте його в будь-якій формі іншим особам. Розгляньте використання додаткових засобів захисту, таких як ключі безпеки (наприклад, фізичні USB-ключі або використання телефону як ключа), щоб знизити ризик компрометації акаунту.

Сумнівні сповіщення та повідомлення. Якщо отримали SMS-повідомлення або електронного листа, який здається підозрілим, не переходьте за посиланням відразу. Наприклад, SMS може прийти не з номера телефону, а з електронної адреси – це може бути ознакою фішингу. У випадку сумнівів відвідайте офіційний сайт безпосередньо і зв'яжіться зі службою підтримки, щоб переконатися у справжності повідомлення.

Фішингові атаки часто використовують OSINT для збору інформації та маніпуляцій із жертвами.

OSINT – це Open Source Intelligence, розвідка на основі відкритих джерел. Такими джерелами переважно виступають соціальні мережі Instagram, Facebook. Останнім часом дуже популярний TikTok.

Джерела OSINT поділяються на кілька основних категорій:

– *ЗМІ* – друковані газети, журнали, радіо та телебачення;

– *Інтернет* – блоги, соцмережі (Facebook, Twitter, Instagram), відеохостинги (YouTube), вікі-довідники та інші онлайн-ресурси, які вирізняються доступністю та актуальністю;

– *державні дані* – звіти, бюджети, слухання, прес-конференції, урядові вебсайти та виступи;

– *академічні публікації* – статті, наукові роботи, дисертації, матеріали конференцій;

– *комерційні дані* – фінансові звіти, бази даних, промислові оцінки;

– *сіра література* – технічні звіти, патенти, робочі документи, бюлетені.

Існує кілька онлайн-сервісів для пошуку інформації за невідомим номером телефону, одним із яких є X-Ray Contact. Сайт дозволяє ідентифікувати власника номера, переглядати його профілі у соціальних мережах та іншу загальнодоступну інформацію.

Щоб уникнути несанкціонованого розповсюдження номера, варто уникати публікації його у відкритих джерелах, використовувати налаштування конфіденційності в соціальних мережах, а також бути обережним із додатками та сайтами, які запитують доступ до контактів.

Один з підвидів OSINT є GEOSINT, який фокусується на зборі та аналізі інформації з відкритих джерел із геопросторовим компонентом. За допомогою GEOSINT можна взнати локацію місця фотографії, по орієнтирах, тіні, та навіть громадського транспорту.

Для GEOSINT здебільшого використовується:

– *geospy.ai* але не завжди кореткно;

– *SunCalc* щоб уточнити місце фото по тіні якщо відомий час;

– *Soar* – платформа дозволяє переглядати, завантажувати, відкривати та взаємодіяти з величезною бібліотекою високоякісних карт та зображень, кожна карта, супутникове зображення та зображення з дронів, які колинебудь існували або будуть існувати, зібрані в одному місці;

– *Online Protractor* – прозорий онлайн транспортир, допоможе вам виміряти кути на зображенні, зробивши знімок і завантаживши його, а потім перетягнувши середню точку транспортира до вершини кута, може збільшувати, зменшувати, обертати і переміщати положення.

Також при аналізі фото варто звертати увагу на об’єкти місцевості, громатський транспорт за маршрутом якого можна ідентифікувати локацію фото.

Щоб уникнути ідентифікації вашої адреси злочинцями, не викладайте у відкритий доступ фотографії з видом з вікна, на яких можна розпізнати місцевість. Уникайте публікації зображень, що містять номери будинків, дорожні знаки, вказівники або інші характерні орієнтири, які можуть допомогти визначити ваше місцезнаходження. Також варто звертати увагу на метадані (EXIF-дані) фотографій, які можуть містити геолокаційні координати – перед публікацією їх слід видаляти.

Висновки. Безпека в інтернеті вимагає уважності та використання сучасних технологій для протидії загрозам. Уникнення публікації конфіденційної інформації у відкритих джерелах, перевірка сумнівних запитів і використання двофакторної аутентифікації – це ключові кроки для захисту персональних даних.

Інформаційні джерела

1. Легомінова С., Щавінський Ю., Рабчун Д., Запорожченко М., & Будзинський О. (2024). Небезпека інструментів osint та способи пом'якшення наслідків їх використання для організації. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), С. 294–303. URL: https://doi.org/10.28925/2663-4023.2024.25.294303

2. Главацька А., Ангельська О., & Опірський І. (2024). Дослідження технології використання osint як нової загрози з деанонімізації особи в інтернет просторі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), С. 19–50. URL: https://doi.org/10.28925/2663-4023.2024.25.1950

3. X-Ray people search engine. URL: https://x-ray.contact/sign-up/

4. ESET. Дослідження на основі відкритих джерел або OSINT: де використовується та в чому небезпека. URL: https://www.eset.com/ua/about/newsroom/blog/ business-security/issledovaniye-na-osnove-otkrytykh-istochnikov-ili-osint-gde-ispolzuyetsya-i-v-chem-opasnost/

5. Wikipedia. Розвідка на основі відкритих джерел.

6. JIGSAW. Безпечніший Інтернет означає безпечніший світ. URL: https://jigsaw.google.com/

7. Тест "Ви вмієте розпізнавати фішинг? ". Розробник: Jigsaw. URL: http://surl.li/lubcix

8. OSINT для журналістів: із чого почати та чим користуватися. URL: http://surl.li/pmldna

9. Інструменти OSINT: GEOINT. URL: http://surl.li/muhgfp

Напрям 5

ГЕНДЕР У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 004.838

ГЕНДЕР У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Надія ЯХНО
Василь ЛУЧИК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *Gender in information security is an important issue that is becoming increasingly important in the context of the digitalization of society. The traditional inequality in the representation of women in this area creates an imbalance that negatively affects the effectiveness of cybersecurity. Diversity of perspectives and gender equality contribute to innovation, improving the protection of information systems and creating a socially just environment. Research shows that women have stronger leadership qualities and a greater tendency to adhere to security policies, which makes them valuable specialists in the field of cybersecurity. Overcoming gender inequality requires educational, cultural and technological initiatives, as well as international cooperation. This will ensure an inclusive environment, increase the effectiveness of cybersecurity and contribute to the involvement of more women in this important field.*

Keywords: *gender equality, information security, cybersecurity, innovation, diversity, women in technology, social justice, inclusivity, security policy, gender imbalance.*

Анотація. *Гендерний аспект у сфері інформаційної безпеки є важливим питанням, яке набуває дедалі більшого значення в умовах цифровізації суспільства. Традиційна нерівність у представленості жінок у цій сфері створює дисбаланс, який негативно впливає на ефективність кіберзахисту. Різноманітність точок зору та гендерна рівність сприяють інноваціям, покращенню захисту інформаційних систем і створенню соціально справедливого середовища. Дослідження показують, що жінки мають сильніші лідерські якості та більшу схильність дотримуватися політик безпеки, що робить їх цінними фахівцями в галузі кібербезпеки. Подолання гендерної нерівності вимагає освітніх, культурних і технологічних ініціатив, а також міжнародного співробітництва. Це забезпечить інклюзивне середовище, підвищить ефективність кібербезпеки та сприятиме залученню більшої кількості жінок до цієї важливої галузі.*

Ключові слова: *гендерна рівність, інформаційна безпека, кібербезпека, інновації, різноманітність, жінки в технологіях, соціальна справедливість, інклюзивність, політика безпеки, гендерний дисбаланс.*

Гендерний аспект у сфері інформаційної безпеки є важливою темою, яка привертає дедалі більше уваги на тлі зростаючої цифровізації суспільства. Ця галузь традиційно вважається переважно чоловічою, що призводить до певного дисбалансу у складі фахівців та управлінських команд. Різноманітність точок зору й досвіду відіграє ключову роль у підвищенні ефективності кіберзахисту та кращому розумінні загроз. Включення гендерної рівності та заохочення жінок до участі у сфері кібербезпеки сприяють не лише соціальній справедливості, але й збільшують потенціал для інновацій та розробки більш ефективних підходів до захисту інформаційних систем.

Участь жінок у сфері кібербезпеки помітно зростає. Згідно з прогнозами CyberCrime Magazine, до 2025 року вони складатимуть 30% світової робочої сили з кібербезпеки, а до 2031 року цей відсоток зросте до 35%. Крім того, зростає кількість жінок, які обіймають керівні посади в галузі, причому 17% жінок займають позиції CISO в компаніях зі списку Fortune 500. За даними Harvard Business Review, жінки мають вищі лідерські якості, ніж чоловіки, що робить їх придатними для відповідальних ролей у ніші кібербезпеки [1].

Гендерні відмінності у сприйнятті технологій стали більш вираженими серед старших працівників і менш вираженими серед молодих працівників. Декілька досліджень показують, що стать пов’язана зі ступенем стурбованості конфіденційністю в Інтернеті, і жінки виявляють більше стурбованості конфіденційністю, ніж чоловіки. Стать значною мірою впливає на наміри співробітників щодо дотримання політики, і жінки мають більші наміри щодо дотримання політики, ніж чоловіки. Чоловіки мають нижчі наміри дотримуватися політики безпеки порівняно з жінками, і пропонує практикам звернути увагу на гендерні відмінності щодо дотримання політики безпеки в організаціях [2].

Подолання гендерної нерівності у сфері інформаційної безпеки є важливим завданням, яке потребує комплексного підходу. Одним з ключових аспектів є розширення освітніх програм, які спрямовані на заохочення дівчат та жінок до вивчення інформаційної безпеки. Важливо створювати програми, що надають стипендії та гранти, а також популяризувати успішні приклади жінок-лідерів у цій галузі, щоб молоді дівчата могли бачити реальні рольові моделі. Залучення дівчат шкільного віку до технічних наук через майстер-класи, тренінги та конкурси також є важливим кроком.

Підвищення обізнаності про важливість гендерної рівності та боротьба з упередженнями через антидискримінаційні кампанії та формування інклюзивної культури в організаціях також є ключовими. Інклюзивна культура підтримує різноманітність та інклюзивність, що сприяє ефективній роботі колективу.

Технологічні ініціативи також можуть відігравати важливу роль у подоланні гендерних упереджень. Використання алгоритмів, що враховують гендерний фактор, і створення спеціалізованого програмного забезпечення

для захисту від гендерно обумовлених кіберзагроз допомагають забезпечити рівність. Міжнародне співробітництво у цій галузі може сприяти обміну найкращими практиками та ідеями, підтримуючи глобальні проекти та ініціативи, спрямовані на подолання гендерної нерівності.

Подолання гендерної нерівності у сфері інформаційної безпеки є важливим завданням, що потребує комплексного підходу. Освітні, культурні та соціальні ініціативи можуть допомогти залучити більше жінок до цієї важливої галузі, підвищуючи її ефективність та інноваційність, а також створюючи більш інклюзивне та рівноправне середовище [3, 4].

Щоб усунути гендерний розрив у цьому секторі, вкрай важливо заохочувати більше жінок продовжувати кар'єру в галузі технологій та кібербезпеки. Кар'єра в сфері кібербезпеки є не тільки прибутковою, але й високою винагородою, яка відзначається постійним попитом, задоволенням від роботи та шансом значно вплинути на ландшафт цифрової безпеки. Завдяки ініціативам, подібним до ініціатив, шляхи до сфери кібербезпеки стають дедалі доступнішими та привабливішими, особливо для жінок, які прагнуть проникнути в цю сферу та досягти успіху.

Висновки. Гендерний аспект у сфері інформаційної безпеки є важливим фактором для забезпечення ефективного функціонування та розвитку цієї галузі. Подолання гендерної нерівності сприяє не лише соціальній справедливості, але й підвищує інноваційність та ефективність кіберзахисту завдяки різноманітності точок зору та підходів. Активне залучення жінок до професій у сфері кібербезпеки через освітні програми, менторство та популяризацію успішних прикладів може суттєво змінити ситуацію. Формування інклюзивного середовища в організаціях, впровадження гендерно чутливих політик і підтримка міжнародного співробітництва є необхідними кроками на шляху до рівноправності. Гендерна різноманітність у командах інформаційної безпеки сприяє більшій стійкості до загроз і створює умови для сталого розвитку цифрового суспільства.

Інформаційні джерела

1. International Women's Day: How to Shrink the Gender Gap in Cyber Security. URL: https://www.terranovasecurity.com/blog/shrinking-the-gender-gap-in-cyber-security (дата звернення 19.11.2024).

2. Gender difference and employees' cybersecurity behaviors. URL: https://www. sciencedirect.com/science/article/abs/pii/S0747563216308688 (дата звернення 19.11.2024).

3. Girls Can Hack. URL: https://www.girlscanhack.com/?gad_source=1&gclid=Cj0KCQiAi_G5BhDXARIsAN5SX7qAzGcS1oOndY8q8KIew9NfRUMYtSFif-lnonJmcaDGrjoAQbtOjFoaAoz9EALw_wcB (дата звернення 19.11.2024).

4. The Importance of Bridging the Gender Gap in Cybersecurity. URL: https://www.eccu.edu/blog/cybersecurity/bridging-gender-gap-cybersecurity/ (дата звернення 19.11.2024).

УДК 355.233:316.346.2

ВПЛИВ ВІЙНИ НА ГЕНДЕРНУ ПАРИТЕТНІСТЬ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Юлія ШЕВЦІВ
Емілія КОСТИШИН
Кафедра соціальної роботи, управління та суспільних наук Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The article examines the impact of the war on gender parity in the Armed Forces of Ukraine. The authors analyze the changes that have occurred in the attitude towards women and men in the military during the war, particularly in the context of expanding the role of women in combat units and leadership. The role of gender parity in the effectiveness and morale of the Armed Forces of Ukraine is highlighted, as well as the future prospects for the development of this issue in the context of the ongoing war.*
Keywords: *army, war, gender equality, parity, sexism.*

Анотація. *У статті розглядається вплив війни на гендерну паритетність у Збройних силах України. Авторкии аналізують зміни, які відбулися в ставленні до жінок та чоловіків в армії в умовах війни, зокрема в контексті розширення ролі жінок у бойових підрозділах та командуванні. Висвітлюється роль гендерної паритетності в ефективності та моральному стані Збройних сил України, а також майбутні перспективи розвитку цієї теми в умовах триваючої війни.*
Ключові слова: *армія, війна, гендерна рівність, паритетність, сексизм.*

Протягом останніх десятиліть в Україні відбуваються значні зміни в розумінні та легітимації ґендерних відносин і механізмів забезпечення ґендерної рівності. Їх успішне впровадження та регулювання в суспільстві передбачають утвердження цінності ґендерної рівності не лише в загальному соціумі, а й в окремих інституціях. Це включає, зокрема, недопущення ґендерної дискримінації, забезпечення рівної участі жінок і чоловіків у силових структурах.

Повтомаштабне вторгнення Росії в Україну (24 лютого 2022 року) виявилося потужним каталізатором у прискоренні процесу подолання гендерної нерівності на військовій службі. Станом на січень 2024 року в українській армії служить 45 587 військовослужбовиць, тоді як у 2014 році цей показник становив понад 16,5 тисяч, а у 2023 році – понад 43,4 тисячі. Серед жінок, які зараз є військовими, 13 487 мають статус учасника бойових дій, понад 4000 захисниць перебувають в районі проведення бойових дій. Попри чисельне збільшення кількості жінок в армії, гендерна нерівність в Збройних Силах України залишається серйозною проблемою. У сучасних умовах у силових структурах переважають стереотипи та установки, засновані на патріархальних уявленнях (Davydyuk, O., 2021).

До 2022 р. експерти виділяли найбільш поширені види сексизму у силових

лових структурах: обмеження на виконання бойових завдань, перешкоди у доступі до високих керівних посад, табу у проходженні служби на підводних човнах чи виконання водолазних робіт; стереотипи про "допоміжну/вторинну" роль жінок у війську; неприязнь і дискримінація через стать; сексуальні домагання та експлуатація; нерівні можливості кар'єрного зростання; упередженнями щодо їхньої здатності виконувати професійні обов'язки через материнство тощо.

Результати національного опитування, проведеного після 2023 р. вказують на те, що люди, які підтримують загальні стереотипи та вважають, що жінки зазнають дискримінації в ЗСУ, частіше мають упереджене ставлення до служби жінок в армії. Більшість респондентів вважають, що жінки здатні командувати бойовими підрозділами, але зазнають більше труднощів у кар'єрному зростанні порівняно з чоловіками. Однак у суспільстві все ще зберігаються стереотипи щодо жінок у ЗСУ: понад половина опитаних вважають, що жінкам краще виконувати небойові завдання, а 40% погоджуються з тим, що жінки-військовослужбовиці мають більші проблеми в родинах, ніж цивільні жінки. Загалом, чоловіки менш схильні вбачати дискримінацію та нерівність між чоловіками і жінками в ЗСУ. Ті, хто підтримує "традиційні" цінності, частіше схильні до стереотипів щодо жінок, вважають за потрібне проводити позитивну дискримінацію та розділяти роль жінок у армії, залишаючи їм "жіночі" обов'язки, поза бойовим досвідом. Водночас серед опитуваних не було виявлено явних сексистів. Однак ефект "збільшуваного скла" (коли відмінності між чоловіками та жінками сприймаються більшими, ніж вони є насправді) все ще має місце (Дискримінація, 2023).

Війна внесла зміни до гендерної паритетності в армії. На сьогодні скасовано офіційні обмеження для військовослужбовців щодо доступу до всіх посад. Жінки мають можливість служити у бойових спеціальностях, таких як гранатометниця, снайперка, артилеристка. Проте існують обмеження на прийом на офіцерські посади, пов'язані з використанням бойових патронів та виконанням водолазних робіт, посади на підводних човнах і надводних кораблях, у керівництві бригадами надводних кораблів, у підрозділах пожежогасіння, де необхідне непряме гасіння пожеж, а також у підрозділах тилового забезпечення, де передбачене використання вибухонебезпечних матеріалів (Бондарчук Н. В., Кравчук І. І., 2024). Проте, жінки-військовослужбовиці нарікають на відсутність спеціальної жіночої форми (тільки серпні 2024 р. Міністерство оборони України затвердило зразок-еталон літнього польового костюма для військовослужбовиць), взуття, касок та бронежилетів, а також проблеми, що виникають у військових умовах, зокрема, відсутність зручностей для особистої гігієни (*Дискримінація, 2023).*

Висновки. Для просування гендерної паритетності у секторі оборони пропонуємо: інтегрувати гендерний компонент в усі рівні освіти; започаткувати посаду Уповноваженої у справах військової служби жінок (за основу взяти досвід Збройних Сил Республіки Польща); вивчати досвід держав, що

мають давню історію включення жінок в армію (Данія, Норвегія, Польща, Туреччина, Канада, США, Ізраїль).

Інформаційні джерела

1. Davydyuk O. O. (2021). Intehratsiia zhinok do sylovykh struktur v Ukraini: sotsiolohichnyi vymir [Integration of Women Into Law Enforcement Agencies in Ukraine: the Sociological Dimension]. Demohrafiia ta sotsialna ekonomika – Demography and Social Economy, 4 (46), pp. 116–133. URL: https:// doi.org/10.15407/dse2021.04.116.

2. Дискримінація різних соціальних груп у ЗСУ: погляди військових та цивільних громадян. (Березень-квітень 2023). URL: https://veteranfund.com.ua/analitics/social-group-discr/

3. Бондарчук Н. В., Кравчук І. І. (2024). Правове забезпечення гендерної рівності у Збройних Силах України. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. Випуск 82: частина 2. С. 15–20. URL: https://doi.org/10.24144/ 2307-3322.2024.82.2.2

УДК 316.346.2

ПОНЯТТЯ ПРО ГЕНДЕРНІ СТЕРЕОТИПИ ТА ЇХ ВПЛИВ НА ПОВСЯКДЕННЕ ЖИТТЯ ЛЮДЕЙ

Роман ЯРЕМКО
Оксана ТКАЧИК
Кафедра практичної психології та педагогіки Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *These theses explore the nature of gender stereotypes and their impact on various aspects of social and personal life. They examine key types of gender stereotypes and their role in sustaining social hierarchies, fostering discrimination, and contributing to gender-based violence. Special attention is given to how stereotypical thinking affects mental health and influences individual behavior in society. The theses also discuss practical ways to challenge and overcome gender stereotypes, aiming to create a more equitable society and improve the well-being of all its members.*

Keywords: *gender stereotypes, gender equality, social roles, discrimination, societal norms.*

Анотація. *Тези присвячені аналізу природи гендерних стереотипів та їхнього впливу на різні аспекти суспільного і особистого життя. Розглянуто основні типи гендерних стереотипів та висвітлено їхнє значення в контексті закріплення соціальної ієрархії, дискримінації та гендерно зумовленого насильства. Окрему увагу приділено наслідкам стереотипного мислення для психологічного здоров'я та впливу на поведінку індивіда у соціумі. Також, проаналізовано шляхи подолання гендерних стереотипів задля змін у суспільстві на краще та добробуту для всіх його членів.*

Ключові слова: *гендерні стереотипи, гендерна рівність, соціальні ролі, дискримінація, суспільні норми.*

Гендерні стереотипи зазвичай розглядаються в негативному контексті, оскільки вони впливають на формування помилкових переконань та настанов, які сприяють дискримінації й насильству. За визначенням Ліппмана, стереотипи є "образами в нашій голові" [1, 317 ст.], що формують сприйняття реальності та визначають очікування від поведінки людей. Утім, хоча стереотипи виконують функцію когнітивного спрощення, полегшуючи процес осмислення складної реальності, вони призводять до серйозних негативних наслідків на соціальному та індивідуальному рівнях. Завдяки спрощенню когнітивних процесів стереотипи сприймаються автоматично, що дозволяє уникнути складного аналізу. Це знижує готовність індивіда до критичного переосмислення переконань і веде до закріплення стереотипного мислення, роблячи його майже "не підвладним" свідомому контролю.

Значення гендерних стереотипів є особливо важливим, оскільки вони визначають соціальні ролі та моделі поведінки, закріплюють соціальну ієрархію та розподіляють ресурси й можливості між чоловіками та жінками. Гендерні стереотипи формують очікування від чоловіків і жінок у різних соціальних, професійних і сімейних контекстах [4, 70 ст.]. В основі цих уявлень лежать штучні конструкції, зумовлені історичними, культурними й релігійними чинниками, які часто сприймаються як "природні" характеристики статі. Стереотипи укорінюються через вплив сімейного середовища, освітніх установ, засобів масової інформації та культури загалом, створюючи тверді очікування щодо поведінки чоловіків і жінок.

Виділяють кілька основних груп гендерних стереотипів [2]:

– стереотипи маскулінності та фемінінності;

– стереотипи щодо розподілу сімейних та професійних ролей;

– стереотипи щодо змісту праці.

Наприклад, стереотипи, що зображають жінок як об'єкти для задоволення чоловічих бажань, формують культуру об'єктивації та приниження жіночої особистості. Це особливо характерно для медійних образів, представлених у рекламі, кіно та телебаченні, де жінок часто зображують як "пасивних об'єктів". Унаслідок цього поширюється культура знецінення жінок і виправдання насильницької поведінки щодо них, а суспільство нерідко сприймає сексуальні домагання або інші форми насильства як природну поведінку чоловіків щодо жінок. Або, для прикладу, стереотип про "чоловіки не плачуть" формує в суспільстві небезпечну установку, яка табуює прояв емоцій чоловіками, особливо таких, як сум, страх, вразливість. Ідея про те, що сльози та емоційна виразність є ознаками слабкості, примушує чоловіків до емоційного придушення з раннього віку, що негативно позначається на їхньому психічному здоров'ї та соціальній поведінці.

Україна, прагнучи інтеграції до Європейського Союзу, зобов'язана дотримуватись принципів гендерної рівності, що є однією з ключових засад політики ЄС [5]. Важливим кроком у цьому напрямку є усунення гендерних стереотипів та формування культури рівноправ'я.

Гендерні стереотипи створюють фундамент для нерівності та гендерно зумовленого насильства. Вони обмежують свободу вибору, спричиняють тиск на індивідів для відповідності соціальним ролям та стають основою для дискримінаційних практик, що мають серйозні психологічні й фізичні наслідки. Подолання гендерних стереотипів потребує зусиль як на рівні окремої людини, так і на рівні суспільства, для того, щоб кожен мав свободу вибору і можливість для самореалізації.

Висновки. Ключовими шляхами подолання гендерних стереотипів є освіта та підвищення обізнаності, зокрема через програми з гендерної рівності у школах та інформаційні кампанії в суспільстві. Важливо змінити підходи у вихованні дітей, підтримуючи їхні інтереси незалежно від статі. У професійній сфері необхідно забезпечити рівні можливості, справедливий найм і гнучкі графіки. Необхідна зміна культурних стандартів, а також аналіз даних про гендерну рівність для контролю ситуації.

Інформаційні джерела

1. Гаврилів О. (2013). Освічений,але пиячить. До питання національних стереотипів. Вісник Львівського університету, (33).

2. Засади розуміння гендеру та гедерної рівності. (2020). URL: https://dsns.gov.ua/upload/9/5/8/0/2020-5-20-112-lekciya-1.pdf

3. Михайлецька А. Ю., Яремко Р. Я. (2024). Статеве виховання як елемент розвитку особистості підлітка. У Особистість в екстремальних умовах: матеріали XI Всеукраїнської науково-практичної конференції – С. 208–210.

4. Саєнко Ю. І., Амджадін Л., & Васильчук М. (2007). Гендерні стереотипи та ставлення громадськості до гендерних проблем в українському суспільстві.

5. Стороженко К. Р., & Гребньов Г. В. (2023). Гендеровані проблеми в українському медіапросторі. UNIVERSUM, (1).

УДК 614.84:316.346.2
ГЕНДЕРНІ ВІДМІННОСТІ У ПІДГОТОВЦІ РЯТУВАЛЬНИКІВ

Ігор КОВАЛЬ
Вікторія ЛАКІШ
Факультет психології та соціального захисту Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The article examines the issue of gender equality in the field of civil protection, focusing on stereotypes that limit women's participation in this profession. It emphasizes that overcoming stereotypes and integrating gender equality contribute to enhancing professional competence, improving team interaction efficiency, and increasing societal trust in rescue services. The integration of gender equality in rescue services is highlighted as a strategic step toward strengthening the professional capabilities and resilience of the State Emergency Service of Ukraine.*

Keywords: *stereotype, gender differences, training, rescuers, equality.*

Анотація. *У статті досліджується проблема гендерної рівності у сфері цивільного захисту, зокрема стереотипи, які обмежують участь жінок у цій професії. Наголошено, що подолання стереотипів та інтеграція гендерної рівності сприяють підвищенню професійної компетентності, ефективності командної взаємодії та загального рівня довіри суспільства до рятувальних служб. Вказано, що інтеграція гендерної рівності у рятувальних службах є стратегічним кроком для зміцнення професійної спроможності та стійкості ДСНС України.*

Ключові слова: *стереотип, гендерні відмінності, підготовка, рятувальники, рівність.*

Стереотип про те, що рятувальниками можуть бути тільки фізично сильні чоловіки, обмежує доступ жінок до цієї професії. Це ігнорує важливі якості, які можуть бути притаманні жінкам, *наприклад*, емоційний інтелект, уважність і здатність до співпраці. Розподіл професійних ролей часто піддається гендерним стереотипам: жінки розглядаються як "ніжні", а чоловіки – як "сильні", що призводить до дисбалансу в розподілі обов'язків і обмежує можливості жінок у ризикованих операціях. Такі суспільні очікування посилюють тиск на жінок-рятувальниць і впливають на їхній стан. У зв'язку з цим, впровадження гендерної рівності і безбар'єрності є ключовими пріоритетами Державної служби України з надзвичайних ситуацій [1].

Соціальні виклики, з якими стикаються чоловіки і жінки, залежать від багатьох різних факторів: культури, соціальних умов, економічної ситуації, віку і рівня освіти. Однак, окрім загальних труднощів, таких як соціальні очікування, насильство, дискримінація, баланс роботи і особистого життя, здоров'я і економічні питання, є і специфічні проблеми для кожної статі. Жінки часто стикаються з гендерною нерівністю, що проявляється в нижчій оплаті праці, обмеженій представленості на керівних посадах і сексуальних домаганнях. Крім того, на жінок часто лягає подвійне навантаження через неврахування їхніх домашніх обов'язків. Для чоловіків характерні виклики, пов'язані з тиском на досягнення успіху і утримання сім'ї, а також з труднощами визнання потреби у психологічній допомозі.

Для рятувальників важливу роль відіграє підготовка, яка включає фізичну, технічну, психологічну підготовку та роботу в команді [2, 3]. Основою є фізична витривалість і сила, адже часто доводиться працювати в екстремальних умовах і під значним навантаженням. Також необхідна психологічна підготовка і здатність швидко приймати рішення під тиском, адже в роботі рятувальників постійно присутні стресові та травматичні ситуації. Ключовим у таких умовах є оперативне спілкування в команді, що допомагає уникати помилок у критичних ситуаціях. Створення інклюзивного середовища в рятувальних службах передбачає гендерну інтеграцію, яка забезпечує рівні можливості для розвитку і для чоловіків, і для жінок. Фізична підготовка повинна враховувати фізичні особливості представників обох статей, щоб навчальні програми були ефективними для всіх. Жінки мають отримувати доступ до спеціального обладнання, що відповідає їхнім фізичним можливостям. Крім того, важливо забезпечити ген-

дерну рівність у доступі до керівних посад, що дозволяє жінкам просуватися кар'єрними сходами і долати бар'єри "скляної стелі".

Проблема гендерної рівності у рятувальних службах є важливою складовою побудови ефективного, інклюзивного та сучасного суспільства. Усунення гендерних бар'єрів і надання рівного доступу до рятувальних професій для чоловіків і жінок дозволяє максимізувати потенціал усіх працівників, залучених до рятувальних операцій. Досвід показує, що команди, у яких враховано різні навички, погляди і підходи, здатні ефективніше реагувати на надзвичайні ситуації та досягати кращих результатів. Гендерна різноманітність не лише покращує комунікацію і командну взаємодію, але й сприяє збільшенню соціальної довіри до рятувальних служб, адже суспільство бачить відображення себе в цих професіях.

Спрямованість на подолання стереотипів та врахування гендерних відмінностей у фізичній і психологічній підготовці сприяє зниженню стресу та підвищенню стійкості рятувальників перед складними викликами. Крім того, впровадження рівних можливостей на керівних посадах дозволяє жінкам розвиватися професійно і не зупинятися на шляху до особистих і кар'єрних досягнень, що важливо для підтримки високих моральних стандартів у команді.

Забезпечення рівного доступу до навчальних програм, адаптованих для чоловіків і жінок, а також створення спеціалізованих програм підтримки під час і після стресових подій, дають можливість розкрити повний потенціал кожного рятувальника. Це також підвищує загальний рівень професіоналізму, що є критично важливим для діяльності ДСНС України і формування позитивного прикладу для суспільства. Рятувальні служби, що приймають і впроваджують гендерну інтеграцію, стають моделлю для інших сфер, показуючи, що гендерна рівність – це не тільки соціальна справедливість, але й спосіб підвищення ефективності та професійної компетентності.

Висновки. Інтеграція гендерної рівності у рятувальних службах є не просто прагненням до справедливості, а стратегічним кроком до зміцнення безпеки, стійкості та професійного розвитку як рятувальних служб, так і суспільства в цілому.

Інформаційні джерела

1. Коваль І. С. Аналіз гендерних стереотипів майбутніх рятувальників у закладі вищої освіти / Психологічні та педагогічні проблеми професійної освіти та патріотичного виховання персоналу системи МВС України : тези доп. наук.-практ. конф., Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2021. 296 с. – С. 96–98.

2. Коваль І. С. Професійно-психологічна підготовка майбутніх рятувальників ДСНС України / Науковий часопис НПУ ім. М. П. Драгоманова. Серія 19 : Корекційна педагогіка та спеціальна психологія. 2015. Вип. 29. – С. 178–183.

3. Koval I. S. Phenomenology of continuous self-development of future rescuers // International scientific conference "The role of psychology and pedagogy in the spiritual development of modern society" : conference proceedings, July 30–31, 2022. Riga, Latvia: "Baltija Publishing", 2022. 364 p., pp. 341–344.

Напрям 6

КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

UDC 004.[021+023+67+9]:519.6

THE MECHANISM OF GENERATING FIBONACCI AND LUCAS POLYNOMIALS

Pavlo GRYTSIUK
Lyubomyr SIKORA
National University "Lviv Polytechnic", Lviv, Ukraine.

Анотація. *Запропоновано механізм генерування поліномів Фібоначчі та Люка, особливість реалізації якого полягає у використанні відповідного рекурентного співвідношення, згідно з яким спочатку необхідно змінну x послідовно помножити на елементи даного полінома, потім потрібно згрупувати схожі доданки з елементами попереднього полінома, внаслідок чого отримаємо елементи наступного полінома.*

Ключові слова: *рекурентне співвідношення, нижня трикутна матриця, шифрування.*

Abstract. *A mechanism for generating Fibonacci and Lucas polynomials is proposed. The feature of its implementation lies in the use of a corresponding recurrence relation, according to which the variable x must first be successively multiplied by the elements of the given polynomial, then it is necessary to group similar terms with the elements of the previous polynomial, as a result of which we obtain the elements of the next polynomial.*

Keywords: *recurrence relation, lower triangular matrix, encryption.*

Fibonacci and Lucas Numbers. Fibonacci numbers are a fundamental mathematical concept that plays an important role in modern computer science and information technologies. Their universality is evident in various fields – from software development to cryptography and financial technologies. Understanding this sequence helps programmers deepen their knowledge in algorithms and data structures, improve their programming skills, and develop more efficient programs.

The Fibonacci sequence is defined by the following recurrence relation:

$$F_{n+1}(x) = xF_n(x) + F_{n-1}(x), \qquad (1)$$

where: $F_0(x) = 0$, $F_1(x) = 1$ for $n \geq 2$. The sequence of Fibonacci numbers *for x = 1* has the form 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10916.. .

Lucas numbers or the Lucas series is an integer sequence named after the mathematician François Édouard Anatole Lucas (1842–1891), who studied both their sequence and the closely related Fibonacci numbers. Lucas numbers and Fibonacci numbers form complementary cases of Lucas sequences.

The Lucas sequence has a similar recurrence relation to the Fibonacci sequence, where each term is the sum of the two preceding terms, but with different initial values. Lucas numbers also have various interrelations with Fibonacci numbers. For example, adding any two Fibonacci numbers separated by two terms in the Fibonacci sequence yields the Lucas number between them.

The Lucas sequence uses the following recurrence relation with different initial values:

$$L_{n+1}(x) = xL_n(x) + L_{n-1}(x), \qquad (2)$$

where $L_0(x) = 2$, $L_1(x) = x$ for $n \geq 2$ і $L_n(x) = F_{n+1}(x) + F_{n-1}(x)$ for $n \in$ □ . The Lucas sequence for $x = 1$ looks like: 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, 2207, 3571, 5778, 9349, 15127, 24476, 39603, 64079, 103682, 167761, 271443... .

Fibonacci and Lucas Polynomials. Fibonacci and Lucas numbers are a popular topic for mathematical enrichment among researchers and their popularization among them. At the same time, various sequences of polynomials called Fibonacci and Lucas polynomials have been in the scientific literature for a long time, as they are closely related, but they have not been as widely studied. These polynomials appear in various areas of application, including data encryption, primarily by the matrix method.

In mathematics, Fibonacci polynomials are a polynomial sequence that can be considered as a generalization of Fibonacci numbers. Polynomials derived analogously from Lucas numbers are called Lucas polynomials [6].

The mechanism for generating Fibonacci or Lucas polynomials involves using the recurrence relation (1) or (2), according to which the variable x must first be multiplied successively by the elements of the given polynomial, then it is necessary to group similar terms with the elements of the previous polynomial, as a result of which we obtain the elements of the next polynomial. For example, given the input polynomials $F_6(x) = x^5 + 4x^3+3x$ and $F_7(x) = x^6 + 5x^4+6x^2 + 1$ the next polynomial will be: $F_8(x) = xF_7(x) + F_6(x) = x(x^6 + 5x^4+6x^2 + 1) + (x^5 + 4x^3+3x) = x^7 + 5x^5+6x^3 + x + x^5 + 4x^3+3x = x^7 + 6x^5+10x^3 + 4x$.

The first few Fibonacci polynomials are:

$$F_0(x)=0; \qquad F_1(x)=1; \qquad F_2(x)=x;$$
$$F_3(x)=x^2+1;$$
$$F_4(x)=x^3+2x;$$
$$F_5(x)=x^4+3x^2+1;$$
$$F_6(x)=x^5+4x^3+3x;$$
$$F_7(x)=x^6+5x^4+6x^2+1;$$
$$F_8(x)=x^7+6x^5+10x^3+4x;$$
$$F_9(x)=x^8+7x^6+15x^4+10x^2+1;$$
$$F_{10}(x)=x^9+8x^7+21x^5+20x^3+5x.$$
… … … …
$$F_{15}(x)=x^{14}+13x^{12}+66x^{10}+165x^8+210x^6+126x^4+28x^2+1;$$
… … … … … …
$$F_{20}(x)=x^{19}+18x^{17}+136x^{15}+560x^{13}+1365x^{11}+2002x^9+1716x^7+792x^5+165x^3+10x.$$

The first few Lucas polynomials are:

$$L_0(x)=2; \qquad L_1(x)=x;$$
$$L_2(x)=x^2+2;$$
$$L_3(x)=x^3+3x;$$
$$L_4(x)=x^4+4x^2+2;$$
$$L_5(x)=x^5+5x^3+5x;$$
$$L_6(x)=x^6+6x^4+9x^2+2;$$
$$L_7(x)=x^7+7x^5+14x^3+7x;$$
$$L_8(x)=x^8+8x^6+20x^4+16x^2+2;$$
$$L_9(x)=x^9+9x^7+27x^5+30x^3+9x;$$
$$L_{10}(x)=x^{10}+10x^8+35x^6+50x^4+25x^2+2.$$

$$L_{0-10}(x)=\begin{pmatrix} 2 \\ x \\ x^2+2 \\ x^3+3x \\ x^4+4x^2+2 \\ x^5+5x^3+5x \\ x^6+6x^4+9x^2+2 \\ x^7+7x^5+14x^3+7x \\ x^8+8x^6+20x^4+16x^2+2 \\ x^9+9x^7+27x^5+30x^3+9x \\ x^{10}+10x^8+35x^6+50x^4+25x^2+2 \end{pmatrix}.$$

Thus, the Fibonacci and Lucas polynomials [2] are a natural extension of the corresponding Fibonacci and Lucas numbers, and therefore many of their properties allow direct proof. The sequence of Fibonacci polynomials and the golden ratio have appeared in many fields of science, including high-energy physics, cryptography, and data coding [1, 5].

Matrix Representation of Lucas Polynomials. Often in mathematical calculations, particularly in the fields of cryptography and data encoding, one has to deal with the matrix representation of Lucas polynomials for the forward process and their inverse form for the reverse process. For this purpose, it is necessary to multiply a special *n*-th order matrix with the appropriate coefficients by an *n*-th degree polynomial, resulting in a set of Lucas polynomials $L_n(x)$ of the corresponding degree. Typically, the special matrix is a lower triangular matrix, all elements of the main diagonal of which are unitary, except for the first one.

To generate Lucas polynomials and their inverse equivalents, a special *n*-th order matrix with appropriate coefficients and an *n*-th degree polynomial must be used. The mechanism for generating Lucas polynomials involves performing a matrix operation of multiplying the special *n*-th order matrix by the *n*-th degree polynomial, resulting in a set of Lucas polynomials from 0-th to *n*-th degree. The mechanism for generating the inverse equivalents of Lucas polynomials involves finding the matrix inverse to the special *n*-th order matrix, and performing the matrix operation of multiplying the inverse *n*-th order matrix by the *n*-th degree polynomial, resulting in a set of inverse Lucas polynomials from 0-th to *n*-th degree.

Below is a set of Lucas polynomials $L_n(x)$ from 0-th to 6-th degree, namely:

$$L_{0-6}(x) = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 4 & 0 & 1 & 0 & 0 \\ 0 & 5 & 0 & 5 & 0 & 1 & 0 \\ 2 & 0 & 9 & 0 & 6 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \\ x^3 \\ x^4 \\ x^5 \\ x^6 \end{pmatrix} = \begin{pmatrix} 2 \\ x \\ x^2+2 \\ x^3+3x \\ x^4+4x^2+2 \\ x^5+5x^3+5x \\ x^6+6x^4+9x^2+2 \end{pmatrix}$$

To obtain the inverse Lucas polynomials, it is necessary to multiply the inverse coefficient matrix by the polynomial, resulting in a set of inverse Lucas polynomials of the corresponding degree $L_n^{-1}(x)$ as follows:

$$L_{0-6}^{-1}(x)=\begin{pmatrix}2&0&0&0&0&0&0\\0&1&0&0&0&0&0\\2&0&1&0&0&0&0\\0&3&0&1&0&0&0\\2&0&4&0&1&0&0\\0&5&0&5&0&1&0\\2&0&9&0&6&0&1\end{pmatrix}^{-1}\begin{pmatrix}1\\x\\x^2\\x^3\\x^4\\x^5\\x^6\end{pmatrix}=\begin{pmatrix}\frac{1}{2}&0&0&0&0&0&0\\0&1&0&0&0&0&0\\-1&0&1&0&0&0&0\\0&-3&0&1&0&0&0\\3&0&-4&0&1&0&0\\0&10&0&-5&0&1&0\\-10&0&15&0&-6&0&1\end{pmatrix}\begin{pmatrix}1\\x\\x^2\\x^3\\x^4\\x^5\\x^6\end{pmatrix}=\begin{pmatrix}1/2\\x\\x^2-1\\x^3-3x\\x^4-4x^2+3\\x^5-5x^3+10x\\x^6-6x^4+15x^2-10\end{pmatrix}.$$

Below is a set of squares of Lucas polynomials $L_n^2(x)$ and their inverse equivalents $L_n^{-2}(x)$ from 0-th to 6-th degree, as follows:

$$L_{0-6}^{2}(x)=\begin{pmatrix}2&0&0&0&0&0&0\\0&1&0&0&0&0&0\\2&0&1&0&0&0&0\\0&3&0&1&0&0&0\\2&0&4&0&1&0&0\\0&5&0&5&0&1&0\\2&0&9&0&6&0&1\end{pmatrix}^{2}\begin{pmatrix}1\\x\\x^2\\x^3\\x^4\\x^5\\x^6\end{pmatrix}=\begin{pmatrix}4&0&0&0&0&0&0\\0&1&0&0&0&0&0\\6&0&1&0&0&0&0\\0&6&0&1&0&0&0\\14&0&8&0&1&0&0\\0&25&0&10&0&1&0\\36&0&42&0&12&0&1\end{pmatrix}\begin{pmatrix}1\\x\\x^2\\x^3\\x^4\\x^5\\x^6\end{pmatrix}=\begin{pmatrix}4\\x\\x^2+6\\x^3+6x\\x^4+8x^2+14\\x^5+10x^3+25x\\x^6+12x^4+42x^2+36\end{pmatrix};$$

$$L_{0-6}^{-2}(x)=\begin{pmatrix}2&0&0&0&0&0&0\\0&1&0&0&0&0&0\\2&0&1&0&0&0&0\\0&3&0&1&0&0&0\\2&0&4&0&1&0&0\\0&5&0&5&0&1&0\\2&0&9&0&6&0&1\end{pmatrix}^{-2}\begin{pmatrix}1\\x\\x^2\\x^3\\x^4\\x^5\\x^6\end{pmatrix}=\begin{pmatrix}1/4&0&0&0&0&0&0\\0&1&0&0&0&0&0\\-\frac{3}{2}&0&1&0&0&0&0\\0&-6&0&1&0&0&0\\\frac{17}{2}&0&-8&0&1&0&0\\0&35&0&-10&0&1&0\\-48&0&54&0&-12&0&1\end{pmatrix}\begin{pmatrix}1\\x\\x^2\\x^3\\x^4\\x^5\\x^6\end{pmatrix}=\begin{pmatrix}1/4\\x\\\frac{2x^2-3}{2}\\x^3-6x\\\frac{2x^4-16x^2+17}{2}\\x^5-10x^3+35x\\x^6-12x^4+54x^2-48\end{pmatrix}.$$

Information sources

1. Esmaeili M., & Esmaeili M. (2010). A Fibonacci-polynomial based coding method with error detection and correction. Computers and Mathematics with Applications, 60, pp. 2738–2752. URL: https://doi.org/10.1016/j.camwa.2010.08.091

2. Falcon S., & Plaza A. (2009). On k-Fibonacci sequences and polynomials and their derivatives. Chaos, Solitons and Fractals, 39, No. 1, pp. 1005–1019. URL: https://doi.org/10.1016/j.chaos.2007.03.007

3. Hoggat V. E. (1969). Fibonacci and Lucas numbers. Palo Alto (CA): Houghton-Mifflin. URL: https://www.peliti.org/Notes/fibonacciLucas.pdf

4. Stakhov A., & Rozin B. (2005). Theory of Binet formulas for Fibonacci and Lucas p-numbers. Chaos, Solitons and Fractals, 27, No. 5, pp. 1162–1177. URL: https://doi.org/10.1016/j.chaos.2005.04.106

5. Koshy Th. (2001). Fibonacci and Lucas Numbers with Applications. John Wiley and Sons, New York, 654 p. URL: https://doi.org/10.1002/9781118033067

6. Jin Z. (2018). On the Lucas polynomials and some of their new identities. Adv Differ Equ, 126 (2018). URL: https://doi.org/10.1186/s13662-018-1527-9

УДК 004.056:004.75

DATA ENCRYPTION ALGORITHMS IN MASS SERVICE SYSTEMS

G. WEIGANG
K. MYRONCHUK
National University of Life and Environmental Sciences of Ukraine.

Анотація. *Алгоритми шифрування в системах масового обслуговування забезпечують безпеку передачі та зберігання даних. Використання AES, RSA, і ECC захищає інформацію від несанкціонованого доступу, що є критичним для сервісів, IoT і платіжних систем та інтелектуальних транспортних систем.*
Ключові слова: *шифрування, безпека даних, AES, RSA, ECC, інтелектуальні транспортні системи.*

Abstract. *Data encryption algorithms in mass service systems ensure the security of data transmission and storage. The use of AES, RSA, and ECC protects information from unauthorized access, which is critical for services, IoT, payment systems, and intelligent transport systems.*
Keywords: *encryption, data security, AES, RSA, ECC, intelligent transport systems.*

The implementation of data encryption in mass service systems is crucial for protecting data integrity and confidentiality, especially given the increasing amount of sensitive information being processed [1]. Numerous algorithms and frameworks have been refined to improve encryption methodologies, regulate encryption configurations, and maximize operational efficiency. Subsequent studies outline the key elements of data encryption algorithms as they pertain to mass service systems [2].

The aim of the study is to analyze and evaluate the effectiveness of modern data encryption algorithms in mass service systems to ensure information security and confidentiality, as well as to develop recommendations for their use, considering the specifics of big data and IoT.

Research Objectives

– Conduct a review of modern approaches to data encryption in mass service systems, including centralized frameworks for encryption management.

– Investigate advanced encryption algorithms, such as modified versions of DES and others that enhance resistance to cryptanalysis.

– Develop recommendations for the optimal selection and implementation of encryption algorithms in mass service systems, depending on data specifics and infrastructure.

In mass service systems, it is crucial to maintain a balance between security, algorithm speed, and hardware requirements. The main types of algorithms used are shown in Figure 1.

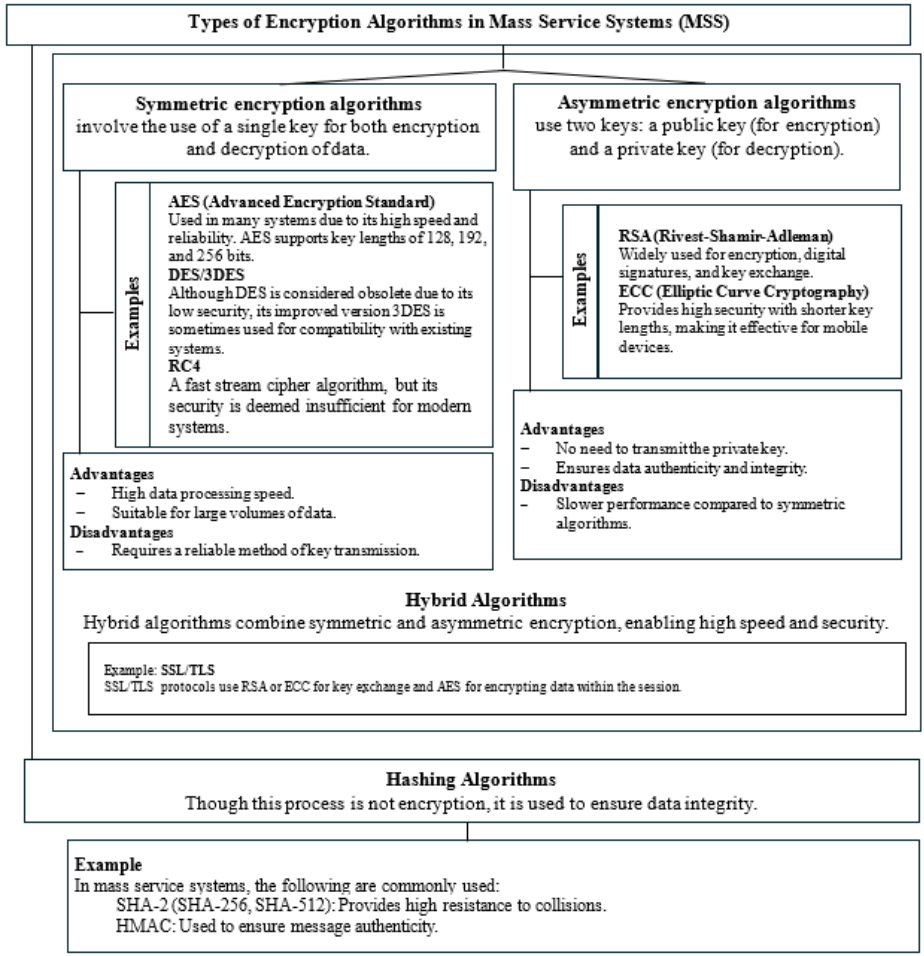


Figure 1 – Main Types of Algorithms

Research on improving the efficiency of encryption algorithms considering fault tolerance criteria should begin with an analysis of the main challenges in such systems [2, 3].

Improving the efficiency of encryption algorithms with respect to fault tolerance involves analyzing the key challenges facing modern systems. One of the main factors is the speed of the algorithms, as systems with high request volumes require solutions that ensure minimal delays. Scalability is also essential, allowing for the processing of large data volumes and supporting an remains a priority, as contemporary threats such as man-in-the-middle attacks or quantum attacks demand

the implementation of innovative and reliable cryptographic methods increasing number of users. Compatibility with legacy systems is another critical aspect since many modern infrastructures require the support of older technologies.

The analysis of advanced encryption algorithms, particularly modified versions of DES, to enhance resistance to cryptanalysis and assess their effectiveness in modern systems involves several stages illustrated in Figure 2.

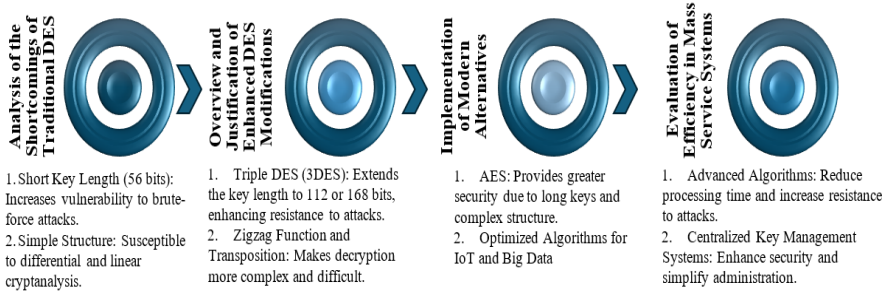


Figure 2 – Analysis of DES in Mass Service Systems

The analysis of traditional DES helped identify the main principles of operation and the structure of encryption rounds, the use of subkeys, and S-boxes [4]. Here is a list of DES vulnerabilities to attacks, such as brute-force attacks, differential cryptanalysis, and linear cryptanalysis. The process of modifying the DES algorithm aimed to enhance its resistance to modern cryptanalysis methods by implementing improved versions [5].

One of the key solutions was the use of Triple DES (3DES), which applies three sequential encryptions to overcome key length limitations, significantly increasing cryptographic strength. Another improvement was DES with a zigzag function, which adds permutation steps, making decryption more difficult for cryptanalysts. Additionally, a column transposition technique was implemented to change the block structure, providing improved diffusion and increasing the algorithm's resistance to attacks. These measures significantly strengthened the protective characteristics of DES in modern conditions.

In the course of the research, we examined modern alternatives and their comparison with DES, specifically analyzing AES (Advanced Encryption Standard) as a modern replacement for DES in many systems and comparing the performance, energy efficiency, and security level of the improved DES with AES and other algorithms [4, 5].

Improved modifications of the DES algorithm were aimed at enhancing cryptographic strength and efficiency in modern conditions. Triple DES (3DES) significantly enhances protection by extending the key to 112 or 168 bits, making the algorithm more resistant to attacks. The use of the zigzag function and transposition improves data diffusion and complicates the decryption process.

Alongside DES improvements, modern mass service systems often use AES (Advanced Encryption Standard), which provides a higher level of security due to longer keys (128, 192, 256 bits) and a complex structure. AES is particularly suitable for processing large data sets and IoT environments, as it is optimized for GPU processing [6–8]. Testing these algorithms in mass service systems demonstrates a reduction in data processing time and increased resistance to modern attacks. Additionally, the use of centralized key management systems contributes to increased data security and simplifies administration.

Conclusions. Thus, the study established that modifications of the DES algorithm can be effectively applied in environments with moderate performance and security requirements. For critical systems with high risk levels, it is recommended to implement more modern algorithms, such as AES, which provide a higher level of data protection. Improved versions of DES are advisable for processing less critical data, and for protecting sensitive information, it is recommended to combine DES with additional security layers such as TLS and VPN cryptographic protocols. The implementation of GPU-optimized algorithms and the use of transposition increase resistance to attacks with minimal computational overhead. Additionally, integrating key management systems ensures a unified encryption approach in large infrastructures, enhancing data security and simplifying administration.

Information sources

1. Alexandre H., Je W., Heo Y., Zhou A., Alexander A., Assaf B., Gur G. Mass encryption management. 2019.

2. Hemasri S., Kiran S., Ranichitra A., Rajesh Kanna A. Improved Data Encryption Standard Algorithm using Zigzag Scan for Secured Data Transmission // International Journal of Innovative Technology and Exploring Engineering. – 2023. doi: 10.35940/ijitee.f9516.0512623.

3. Dass S. A., Prabhu J. Comparative Analysis of a Systematic Coherent Encryption Scheme for Large-Scale Data Management Using Cryptographic Encryption Technique // Lecture Notes in Electrical Engineering. – 2019. doi: 10.1007/978-981-13-1927-3_46.

4. Zharikov V., Kolesnikov V., & Egorov V. Ciphering the modern world: A comprehensive analysis of DES, AES, RSA, and DHKE [Conference Paper] // International Conference on Information Security and Cryptography. IEEE Xplore, 2023. doi: 10.1109/ICSIC.2023.09348.

5. Agarwal S., & Soni A. Analysis and comparison of DES, AES, RSA encryption algorithms // IEEE Conference Publication. IEEE Xplore, 2021. doi: 10.1109/10073996.

6. Hersans M., Zhi H., & Li T. Centralized framework for encryption management in large-scale systems // Journal of Cryptographic Engineering, 11(2). – pp. 233–245. – 2019. doi: 10.1007/s10586-019-03099-8.

7. Hemasri D., & Kumar S. Enhancement of DES with zigzag functions and transposition techniques // Journal of Cryptography and Security, 42(4). – pp. 287–304. – 2023. doi: 10.1016/j.jocs.2023.06.008.

8. Dass P., & Prabhu A. Coherent encryption algorithm for IoT and multimedia big data security // Journal of Information Security, 10(4). – pp. 345–359. – 2019. doi: 10.1016/j.jinfosec.2019.05.002.

УДК 004.838

КРИПТОГРАФІЧНІ МЕТОДИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Сніжана ЧОРНЕНЬКА
Олександр МАНЖАЙ
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The work examines modern cryptographic methods of information protection, their main principles and characteristics. The advantages and disadvantages of various types of encryption are analyzed, including symmetric and asymmetric cryptosystems, digital signatures, hashing, and key management. The relevance of using cryptography to ensure the integrity, confidentiality and authenticity of information in the digital age is highlighted, as well as the latest challenges associated with the development of quantum technologies are discussed. The work is aimed at improving the understanding of data protection methods in the public, corporate and private spheres.*
Keywords: *cryptography, encryption, information security, symmetric encryption, asymmetric encryption, digital signature, hash function, key management, data protection.*

Анотація. *У роботі розглянуто сучасні криптографічні методи захисту інформації, їх основні принципи та характеристики. Проаналізовано переваги та недоліки різних видів шифрування, включаючи симетричні та асиметричні криптосистеми, цифрові підписи, хешування та управління ключами. Висвітлено актуальність використання криптографії для забезпечення цілісності, конфіденційності та автентичності інформації у цифрову епоху, а також обговорено новітні виклики, пов'язані з розвитком квантових технологій. Робота спрямована на підвищення розуміння методів захисту даних у державних, корпоративних і приватних сферах.*
Ключові слова: *криптографія, шифрування, інформаційна безпека, симетричне шифрування, асиметричне шифрування, цифровий підпис, хеш-функція, управління ключами, захист даних.*

В епоху інформаційних технологій питання захисту інформації стає надзвичайно актуальним. Із швидким розвитком цифрових комунікацій та глобалізацією даних, що передаються через мережу Інтернет, виникає значна потреба у надійних методах забезпечення безпеки інформації. Криптографія як наука про шифрування даних відіграє ключову роль у захисті інформації, адже вона дозволяє забезпечити цілісність, автентичність та недоступність даних для несанкціонованого доступу.

На сьогодні криптографічні методи є основою для захисту інформації в різних сферах: від банківської та фінансової до військової та державної безпеки. Основні криптографічні алгоритми та сучасні методи квантової крип-

тографії, дозволяють створювати ефективні рішення для захисту даних у цифровому середовищі. Однак стрімкий розвиток обчислювальних потужностей та можливе впровадження квантових комп'ютерів ставить перед криптографією нові виклики, адже традиційні методи можуть втратити свою надійність. Метою цієї роботи є аналіз сучасних криптографічних методів захисту інформації.

Криптографічні методи захисту інформації – це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. Криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї. Даний метод захисту реалізується у вигляді програм або пакетів програм [1].

Таблиця 1.

Основні криптографічні методи для захисту інформації

Метод	*Опис*	*Переваги*	*Недоліки*
Симетричне шифрування	Використовує один ключ для шифрування і дешифрування даних.	Висока швидкість шифрування.	Потреба у безпечній передачі ключа між сторонами.
Асиметричне шифрування	Використовує пару ключів: відкритий для шифрування і закритий для дешифрування.	Підвищена безпека передачі даних.	Складніший і повільніший процес шифрування.
Хешування	Перетворює дані в унікальний фіксований рядок, який не можна дешифрувати назад.	Захист паролів та цілісність даних.	Неможливо відновити оригінальні дані з хешу.
Електронний цифровий підпис	Гарантує автентичність та цілісність повідомлень через шифрування хешу закритим ключем.	Забезпечує перевірку автентичності та запобігає підробці.	Потребує використання асиметричної криптографії.
Квантова криптографія	Використовує закони квантової механіки для передачі ключів.	Теоретично абсолютна безпека передачі ключів.	Технологія знаходиться на стадії розвитку і є дорогою.

Захист інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації [3].

Криптографія включає створення та аналіз протоколів, які запобігають доступу третіх осіб до даних. Його основними цілями є конфіденційність: забезпечення доступу до інформації лише тим, хто має на це право; цілісність: забезпечення точності та повноти даних; аутентифікація: перевірка особи користувачів та достовірності повідомлень чи даних; невідмовність: запобігання заперечення людьми своїх дій [2].

Сучасна криптографія включає в себе основні методи для захисту інформації:

Криптосистеми з відкритим ключем. Оригінальний текст шифрується відкритим ключем адресата і передається йому. Зашифрований текст у принципі не може бути розшифрований тим же відкритим ключем. Дешифрування повідомлення можливе тільки з використанням закритого ключа, який відомий тільки самому адресату. Криптографічні системи з відкритим ключем використовують так звані незворотні або односторонні функції, які мають наступну властивість: при заданому значенні x відносно просто обчислити значення $F(x)$, однак якщо $y = F(x)$, то немає простого шляху для обчислення значеннях. Безліч класів незворотних функцій і породжує все розмаїття систем з відкритим ключем [1].

Симетричні криптосистеми. В алгоритмах симетричного шифрування використовується один і той самий ключ для виконання функцій шифрування та дешифрування. Завдяки більшій швидкості симетричне шифрування часто використовують як спосіб захисту даних у багатьох сучасних комп'ютерних системах. *Наприклад*, розширений стандарт шифрування (AES) використовується урядом Сполучених Штатів для шифрування таємної та конфіденційної інформації. Раніше використовувався інший стандарт шифрування даних – DES, який був розроблений у 1970-х роках як стандарт для симетричного шифрування [4].

Асиметричне шифрування. В асиметричних системах ключ, який використовується для шифрування, відомий як публічний ключ, і ним можна поділитися з іншими. А ключ, який використовується для дешифрування, є приватним і його необхідно тримати в секреті. Асиметричне шифрування може застосовуватися в системах, де в багатьох користувачів може виникати потреба шифрування та дешифрування повідомлення чи набору даних, особливо коли швидкість і обчислювальна потужність не є основними проблемами. Одним із прикладів такої системи є зашифрована електронна пошта, в якій публічний ключ можна використовувати для шифрування повідомлення, а приватний ключ – для його дешифрування [4].

У багатьох випадках симетричне та асиметричне шифрування використовуються разом. Типовими прикладами таких гібридних систем є криптографічні протоколи рівня захищених сокетів (SSL) і протоколи захисту транспортного

рівня (TLS), які були розроблені для забезпечення безпечної взаємодії в Інтернеті. Протоколи SSL вже не вважаються надійними, тож їх використання слід припинити. А ось у надійності протоколів TLS сумнівів не виконало, та вони широко використовуються в усіх основних браузерах [4].

Цифровий підпис. Цифрові підписи, що використовуються для перевірки автентичності даних, підтверджують, що дані виходять саме від підписувача і не були змінені. Вони використовуються, *наприклад*, у повідомленнях електронної пошти, електронних документах та онлайн-платежах. Міжнародні стандарти, що визначають схеми цифрового підпису, включають ISO/IEC 9796, ISO/IEC 14888, ISO/IEC 18370 та ISO/IEC 20008 [5].

Криптографічна хеш-функція. Це метод, який перетворює рядок даних будь-якої довжини на хешований результат (хеш-сума вхідних даних) фіксованої довжини. Хеш-функції мають безліч застосувань, *наприклад*, у цифрових підписах, MAC (кодах автентифікації повідомлень) та контрольних сумах (для перевірки пошкодження даних). Міжнародні стандарти, що визначають хеш-функції, включають ISO/IEC 9797-2, ISO/IEC 9797-3 та ISO/IEC10118 [5].

Управління ключами. Це процес системи обробки інформації, який полягає в складанні та розподілі ключів між користувачами. Основні напрямки використання криптографічних методів – передача конфіденційної інформації по каналах зв'язку (*наприклад*, електронна пошта), встановлення автентичності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому вигляді [1].

Висновки. Отже, криптографія дозволяє досягти високого рівня захисту конфіденційності, цілісності та автентичності інформації, що є критичними аспектами для державних і приватних структур, а також для індивідуальних користувачів. Сучасні криптографічні методи, включаючи симетричне і асиметричне шифрування, цифрові підписи, хешування та постійно вдосконалюються для відповіді на нові загрози.

Інформаційні джерела

1. Криптографічні методи захисту інформації. Контроль цілісності програмних та інформаційних ресурсів. URL: http://surl.li/yuyvkb (дата звернення 01.11.2024).

2. Що таке криптографія у блокчейні? URL: https://blog.whitebit.com/uk/what-is-cryptography-in-blockchain/ (дата звернення 01.11.2024).

3. Основні поняття криптографії та захисту інформації. URL: http://surl.li/soedro (дата звернення 01.11.2024).

4. Симетричне та асиметричне шифрування. URL: https://academy.binance.com/uk/articles/symmetric-vs-asymmetric-encryption (дата звернення 01.11.2024).

5. Що таке криптографія? URL: https://www.isoprioritet.com.ua/shho-take-kryptografiya/ (дата звернення 01.11.2024).

УДК 004.056.5:614.2

ЗАСТОСУВАННЯ МЕТОДІВ ШИФРУВАННЯ В СИСТЕМАХ ЗАХИСТУ МЕДИЧНИХ ДАНИХ

***Anna DEMYDOVA*[1]**
***Наталія МАСЛОВА*[2,3]**
***Тарас КІС*[3]**

[1]***Medical Center Medyk, Rzeszow, Poland.***
[2]***Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.***
[3]***Кафедра прикладної математики та інформатики Донецького національного технічного університету, м. Дрогобич, Україна.***

Abstract. *Encryption is one of the most effective methods for protecting healthcare data, as it ensures the confidentiality and integrity of information. Evaluating the effectiveness of encryption methods allows for identifying the most reliable approaches to safeguarding healthcare data and enhancing the overall security level of healthcare systems.*
Keywords: *encryption, protection, healthcare systems, analysis.*

Анотація. *Шифрування є одним із найефективніших методів захисту медичних даних, оскільки забезпечує конфіденційність і цілісність інформації. Оцінка ефективності методів шифрування дозволяє визначити найбільш надійні підходи до захисту медичних даних та підвищити загальний рівень безпеки медичних систем.*
Ключові слова: *шифрування, захист, медичні системи, аналіз.*

Захист медичних даних є критично важливим завданням у сучасних умовах цифровізації охорони здоров'я. Медична інформація містить особисті та конфіденційні відомості, що стосуються здоров'я пацієнтів, діагнозів, методів лікування тощо. Несанкціонований доступ до цих даних або їх витік можуть призвести до серйозних наслідків, таких як порушення конфіденційності, дискримінація, фінансові втрати, а також підрив довіри до медичних установ. Чутливість інформації, яка стосується здоров'я, діагнозів, та лікування пацієнтів, робить ці дані особливо вразливими до різних видів кіберзагроз. Актуальність теми захисту медичних даних за допомогою шифрування обумовлена швидким розвитком цифрових технологій у сфері охорони здоров'я та зростанням обсягу даних медичних систем, які зберігаються та передаються в електронному вигляді.

Мета дослідження – оцінка аналіз застосовності та ефективності шифрування як засобу захисту медичних даних.

Аналіз останніх досліджень та публікацій

Медичні установи дедалі частіше стають ціллю кібератак, несанкціонованого доступу, зловмисних дій. Дослідження, проведені Check point

Software Technologies [1] демонструють, що у першому кварталі 2023 року атаки на сектор охорони здоров'я збільшилися на 22% в порівнянні з минулим періодом та досягли у середньому 1684 атак на тиждень.

Аналіз існуючих підходів до захисту медичних даних показує, що захист базується на комплексному поєднанні технічних, програмних та адміністративних методів, серед яких є шифрування, системи контролю доступу, автентифікація, постійний моніторинг систем та аудит. Інструментарій захисту медичних систем включає застосування блокчейну, технології штучного інтелекту, хмарних рішень. Одним з основних методів захисту медичної інформації як при зберіганні, так і під час передавання є шифрування. Дослідження з застосування методів шифрування у медицині достатньо часто публікуються в оглядах електронної системи здоров'я *Health IT* [2], в роботах Чжан Р., Сюе Р., Лю Л. [3], в огляді [4] й інших матеріалах.

Основна частина

Шифрування відіграє ключову роль у забезпеченні безпеки даних у різних системах охорони здоров'я, допомагаючи захищати конфіденційну інформацію пацієнтів і забезпечуючи контроль доступу.

Так, в системі Електронних медичних записів (Epic Systems, EMR) для захисту даних та під час їх передачі та зберігання застосовуються стандарти шифрування AES. Такі проекти, як *MediBloc* та *Gem Health*, забезпечують безпечний і незмінний спосіб зберігання даних пацієнтів. MediBloc використовує криптографічні методи для захисту особистої інформації пацієнтів, дозволяє здійснювати безпечний обмін даними між медичними установами та пацієнтами. А система IBM Healthcare Encryption застосовує системи гомоморфного шифрування

Методологія оцінки ефективності захисту даних

При оцінці ефективності захисту даних, зокрема в медичних інформаційних системах, використовуються ряд критеріїв, кожен з яких впливає на загальну ефективність захисту даних і вибір конкретного рішення для медичних систем. Розглянемо три критерії, важливі, з нашої точки зору саме для медичних систем: рівень безпеки, продуктивність й простота адміністрування.

Рівень безпеки. Основний критерій ефективності, що визначає здатність системи протистояти загрозам, як-от кібератаки, витоки даних або несанкціонований доступ. Рівень безпеки залежить від застосованих криптографічних методів (*наприклад*, симетричне або асиметричне шифрування), довжини ключа, а також від наявності багаторівневих механізмів аутентифікації.

Продуктивність. Критерій стосується швидкості, з якою система може виконувати операції шифрування та розшифрування. Швидкість обробки важлива, оскільки впливає на зручність використання системи, особливо при обробці великої кількості даних в режимі реального часу, *наприклад*, під час роботи з великими базами пацієнтських даних.

Простота впровадження та адміністрування. Критерій визначає легкість налаштування, управління та підтримки системи захисту даних. Важливо, щоб медичний персонал міг легко керувати системою, а адміністратори могли швидко вносити зміни або налаштовувати нові рівні доступу. Простота впровадження особливо актуальна в умовах обмежених ресурсів, де технічний персонал є допоміжним й працює віддалено.

Наприклад, деякі рішення на основі хмарних технологій, як-от AWS HealthLake, надають готові інструменти для шифрування та управління доступом. Це значно знижує витрати на технічне обслуговування й потребує меншої кількості спеціалістів – адміністраторів з галузі ІТ.

Наведемо порівняльну таблицю (Таблиця 1) основних методів шифрування із врахуванням їх використання у медичних системах. У таблиці проаналізовано п’ять різних методів шифрування, посилання на застосування яких вказано в останній колонці.

Таблиця 1

Методи шифрування у медичних системах

Метод шифрування	*Переваги для медичних систем*	*Недоліки для медичних систем*	*Приклади використання*
Симетричне шифрування (алгоритми AES, DES)	– висока швидкість шифрування;	– складне управління ключами при багатокористувацькому доступі;	Використовується в системах електронних медичних записів (EMR), таких як *Epic Systems* [4]
	– метод зручний для зберігання внутрішніх даних, *наприклад*, записів пацієнтів	– обмежені можливості для зовнішнього обміну даними	
Асиметричне шифрування (наприклад, RSA)	– забезпечує безпеку під час передачі даних між медичними установами.	– низька продуктивність при шифруванні великих обсягів медичних баз даних.	Використовується для захищеної передачі даних у телемедицині та при інтеграції медичних систем [5]
	– застосовний для аутентифікації користувачів.	– розміри ключів збільшують системне навантаження.	
Атрибутивне шифрування (ABE)	– гнучке керування доступом на основі ролей та атрибутів користувачів, застосовується для обміну даними між лікарями.	– висока обчислювальна складність обмежує використання на рівні локальних баз даних;	Застосовується у хмарних платформах, таких як *Microsoft Azure for Healthcare*, для забезпечення контролю доступу [4].
		– адміністрування складне, вимагає висококваліфікованих спеціалістів.	
Гомоморфне шифрування	– підтримує обробку даних у бітовому вигляді, що сприяє конфіденційності;	– має низьку продуктивність з для великими обсягами медичних даних;	Використовується в системах захищеного аналізу великих баз медичних

	– забезпечує захист під час обчислень з персональними даними	– потребує значних обчислювальних ресурсів, складно для впровадження в реальному часі;	даних і клінічних досліджень [5].
Блокчейн з криптографією	– підвищує цілісність медичних записів, знижує ризик маніпуляцій даними;	– не підходить для зберігання великих даних через значні вимоги до пам'ят;	Використовується для управління медичними записами та обміну даними в системах, таких як *Gem Health* [4, 5].
	– забезпечує аудит доступу до медичної інформації.	– складна інтеграція з традиційними медичними системами.	

Кожен із цих методів має свої переваги та обмеження, що робить їх ефективними для певних аспектів захисту медичних даних. *Наприклад*, симетричне шифрування часто використовується для локального зберігання записів пацієнтів, а атрибутивне шифрування – для доступу до хмарних баз. Гомоморфне шифрування, хоч і складне у впровадженні, дозволяє здійснювати обчислення над зашифрованими даними, що важливо для безпечного обміну результатами медичних досліджень.

Висновки. Розвиток цифрових технологій у сфері охорони здоров'я підкреслює актуальність досліджень щодо застосування шифрування для захисту медичних даних. Оцінка ефективності методів шифрування базується на трьох основних критеріях: рівень безпеки, продуктивність і простота впровадження. Високий рівень безпеки забезпечується багаторівневими методами шифрування. Різні методи шифрування мають свої переваги для певних аспектів захисту, що дозволяє адаптувати їх відповідно до специфічних потреб медичних систем.

Інформаційні джерела

1. Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most, Check Point Research, April 27, 2023. URL: https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

2. HealthIT.gov. (2023). Data Encryption and Security in Healthcare. Retrieved from HealthIT.gov.

3. Zhang R., Xue R., Liu L. Security and privacy for healthcare blockchains. IEEE Trans. Serv. Comput. 2021, 15, pp. 3668–3686. [Google Scholar] [CrossRef]. URL: https://ieeexplore.ieee.org/document/9445631

4. Sara Jordan, Clara Fontaine, Rachele Hendricks-Sturrup. Selecting Privacy-Enhancing Technologies for Managing Health Data Use. Review article Front. Public Health, 16 March 2022, Sec. Digital Public Health, Volume 10 – 2022. URL: https://doi.org/10.3389/fpubh.2022.814163. URL: https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2022.814163/full

5. Hamed Taherdoost. Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives. Sci 2023, 5(4), 41. URL: https://doi.org/10.3390/sci5040041

УДК 004.056.55

СУЧАСНІ КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Ольга КОБИЛКІНА
Іван РОВЕЦЬКИЙ
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *In today's digital environment, the volume of data transmitted and stored is constantly growing, which creates new challenges in the field of information security. This work highlights modern cryptographic methods of information protection, which ensure confidentiality, integrity, authenticity and irrefutability of data.*
Keywords: *encryption, cryptography, access, information.*

Анотація. *У сучасному цифровому середовищі обсяг даних, що передаються та зберігаються, невпинно зростає, що створює нові виклики у сфері інформаційної безпеки. Дана робота висвітлює сучасні криптографічні методи захисту інформації, які забезпечують конфіден-ційність, цілісність, автентичність і незаперечність даних.*
Ключові слова: *шифрування, криптографія, доступ, інформація.*

Шифрування, яке є основою сучасної інформаційної безпеки, набуває критичного значення в умовах стрімкого розвитку цифрових технологій. Сучасні реалії вимагають надійних рішень для забезпечення конфіденційності, цілісності та доступності даних. Окрім захисту електронних комунікацій і інформаційних систем, шифрування зміцнює довіру між учасниками цифрового середовища. Обсяг електронного обміну інформацією постійно зростає, тому криптографічні протоколи гарантують захист персональних даних, фінансову безпеку та збереження комерційної таємниці. Завдяки сучасним системам шифрування можна не лише забезпечи-ти захист інформації, але й передбачити потенційні загрози, мінімізуючи ризики несанк-ціонованого доступу до даних.

Криптографія, як наука про захист інформації, постійно розвивається, реагуючи на нові технологічні виклики. Одним з ключових напрямків її еволюції стало удосконалення класичних методів шифрування, а саме симетричні та асиметричні алгоритми.

Симетричні алгоритми шифрування – це методи, у яких один і той самий ключ використовується як для шифрування, так і для розшифрування даних. Основним принципом є спільне володіння ключем між відправником і одержувачем. До основних симетричних алгоритмів шифрування відносяться AES, DES, та ChaCha20.

AES (Advanced Encryption Standard) став міжнародним стандартом через свою ефективність і надійність, так як він підтримує різну довжину ключа: 128, 192, і 256 біт, що робить їх стійкими до злому.

DES (Data Encryption Standard) вважається застарілим через невелику довжину ключа (56 біт).

ChaCha20 став популярним у мобільних додатках завдяки високій швидкості та ефективності в пристроях із низьким енергоспоживанням. ChaCha20 функціонує шляхом створення ключового потоку, який генерується з використанням 256-бітного ключа, 64-бітного nonce (одноразового числа) та 64-бітного лічильника. Цей ключовий потік ком-бінується з відкритим текстом за допомогою побітової операції XOR, що дозволяє отри-мати зашифрований текст (шифротекст). Процес XOR полягає у виконанні операції ви-ключного АБО між ключовим потоком і відкритим текстом, забезпечуючи надійне шифрування та можливість зворотного дешифрування.

Завдяки простоті обчислень симетричні алгоритми є значно швидші, що є особ-ливо важливим для роботи з великими обсягами даних. Також вони потребують менше обчислювальних ресурсів, що робить їх оптимальними для обмежених середовищ, таких як IoT або мобільні пристрої. Сама реалізація симетричних алгоритмів вважається менш складною, що зменшує ймовірність помилок у коді.

Проте, дані методи мають свої обмеження так як обидві сторони повинні мати доступ до одного і того самого секретного ключа, що ускладнює його безпечну передачу та зберігання. Кожна пара користувачів потребує окремий ключ. У великих системах це створює значну кількість ключів, які потрібно управляти через що виникає слабкість у масштабуванні даного методу. Симетричні алгоритми не дозволяють реалізувати функції, які підтверджують автентичність відправника, такі як цифрові підписи і якщо секретний ключ буде скомпрометовано, всі дані, зашифровані цим ключем, стануть доступними для зловмисника.

Асиметричні алгоритми шифрування – це методи, що використовують пару ключів: відкритий ключ для шифрування даних і закритий ключ для їх розшифрування. Відкритий ключ можна вільно поширювати, тоді як закритий має залишатися конфіден-ційним. Цей підхід вирішує проблему безпечного обміну ключами, властиву симетрич-ним методам. До асиметричних алгоритмів шифрування відносяться. RSA, ECC, DSA, там Diffie-Hellman.

RSA (Rivest-Shamir-Adleman) є один із найпоширеніших алгоритмів, заснований на складності факторизації великих чисел та використовується для шифрування даних, цифрових підписів і обміну ключами.

ECC (Elliptic Curve Cryptography) в свою чергу спирається на математичні власти-вості еліптичних кривих. Цей алгоритм забезпечує високу безпеку при менших розмірах ключів порівняно з RSA, що робить його ефективнішим для обмежених середовищ.

DSA (Digital Signature Algorithm) призначений для створення цифрових підписів, що забезпечує автентифікацію та цілісність даних.

Diffie-Hellman- використовується для безпечного обміну ключами через незахи-щені канали.

При використанні асиметричних алгоритмів не потрібно передавати закритий ключ; використовується лише відкритий ключ, який може бути доступний публічно. Один відкритий ключ можна використовувати для взаємодії з багатьма користувачами, що зменшує кількість необхідних ключів. Також асиметричні алгоритми дозволяють створювати цифрові підписи, які підтверджують автентичність відправника та цілісність даних, що використовуються в багатьох сценаріях, таких як шифрування, автентифікація, обмін ключами та цифрові підписи.

Асиметричні алгоритми потребують більше обчислювальних ресурсів так як обчислення в асиметричних алгоритмах значно складніші й повільніші ніж у симетрич-них, що робить їх менш ефективними для шифрування великих обсягів даних, що може бути проблемою для пристроїв із низькою потужністю, таких як IoT. Безпека даних алго-ритмів прямо пропорційна довжині ключа. Для забезпечення стійкості до атак потрібні довгі ключі, що збільшує обчислювальну складність.

Висновки. Із розвитком цифрових технологій і зростанням кількості даних, які передаються та зберігаються в електронному вигляді, шифрування стало критично важливим інстру-ментом для забезпечення конфіденційності, цілісності та доступності інформації. Робота над удосконаленням симетричних та асиметричних алгоритмів є основою розвитку циф-рової безпеки. Вона дозволяє адаптувати криптографію до нових викликів, захищати інформацію в умовах глобалізації та технологічного прогресу, забезпечуючи надійний захист даних для суспільства, бізнесу й урядових структур.

Інформаційні джерела

1. Katz J. and Lindell Y. (2021). Introduction to modern cryptography. Boca Raton, Fl: Crc Press.

2. Stallings W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.

3. Menezes A., van Oorschot P., & Vanstone S. (2019). Handbook of Applied Cryptography. CRC Press.

4. Biryukov A., & Khovratovich D. (2019). Advanced Cryptanalysis of Block Ciphers and Hash Functions. Springer.

УДК 004.056.5:004.421.5

АПАРАТНИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ

Денис ОСТАПЕЦЬ
Володимир ДЗЮБА
Український державний університет науки і технологій, м. Дніпро, Україна.

Abstract. *The paper reviews the principles of developing a system for hardware generation of true random numbers. The structure of the hardware and the interaction protocol between system elements are considered. The hardware and software of the system have been developed. An analysis of the degree of randomness of sequences of numbers obtained in different modes using a set of statistical and visual tests was carried out. Recommendations are provided on the features and evaluation of the effectiveness of the use of hardware generators as part of information protection systems.*

Keywords: *hardware generation, true random numbers, generator, information protection systems.*

Анотація. *У роботі розглянуто принципи розробки системи апаратної генерації випадкових чисел. Розглянута структура апаратної частини та протокол взаємодії окремих елементів системи. Розроблено апаратне та програмне забезпечення системи. Проведено аналіз ступеня випадковості послідовностей чисел, отриманих у різних режимах за допомогою набору статистичних і візуальних тестів. Надано рекомендації щодо особливостей та оцінки ефективності використання апаратних генераторів у складі систем захисту інформації.*

Ключові слова: *апаратна генерація, випадкові числа, генератор, системи захисту інформації.*

В сучасних прикладних науках широко застосовуються випадкові числа. Це такі галузі, як криптографія, захист інформації, статистика, чисельні методи, графіка, комп'ютерні ігри, тестування, імітаційне моделювання і т.і. При цьому, існує два основних підходи для отримання випадкових чисел:

– Генерування псевдовипадкових чисел за допомогою спеціальних алгоритмів або таблиць. При однаковому початковому налаштуванні буде отримано ту саму послідовність чисел. Також, такі послідовності повторюються через певний період. Для використання таких алгоритмів не потрібно додаткове апаратне забезпечення, алгоритми порівняно швидкі та функції генерації присутні у більшості мов програмування високого рівня.

– Використання спеціальних апаратних пристроїв, що генерують істинно випадкові числа та програмного забезпечення, що може працювати з такими пристроями. Для генерування таки пристрої, як правило, використовують шумовий сигнал від одного чи декількох джерел, що оцифровується і отримане значення використовується або для початкового налашту-

вання послідовності псевдовипадкових чисел, або у якості чергового випадкового числа.

– Розробка та дослідження засобів для генерування випадкових та псевдовипадкових чисел є досить актуальною проблемою.

Метою роботи є дослідження якості послідовностей випадкових чисел, отримуваних за допомогою апаратних генераторів істинно випадкових чисел з використанням різних джерел шуму.

В роботі проведено аналіз та вибір джерела шумового сигналу для апаратного генератора істинно випадкових чисел. За його результатами пропонується використання лавинного та атмосферного джерел шуму. Лавинний шум у стабілітронах або спеціалізованих шумових діодах є популярним та недорогим джерелом ентропії. Таке джерело шуму часто використовується в промислових зразках апаратних генераторів випадкових чисел або сигналів. Атмосферне джерело шуму, для отримання якого можна використати радіоприймач, є більш дорогим рішенням, але дозволяє збільшити швидкість генерації випадкових чисел.

Побудовано структуру апаратної та програмної частин. Розроблено протокол взаємодії окремих елементів системи, запропоновані режими генерування випадкових чисел, реалізовано апаратне та програмне забезпечення системи.

В системі можуть використовуватися декілька різних апаратних пристроїв, в т.ч. одночасно. Пристрої можуть використовувати різні джерела шуму. Кожний пристрій підключається до порту комп'ютера за допомогою послідовного інтерфейсу. Взаємодію з кожним пристроєм по інтерфейсу та управління його роботою на боці комп'ютера виконує спеціально розроблене програмне забезпечення – служба генерації випадкових чисел. Прикладні програми для отримання випадкових чисел звертаються до служби.

Для отримання одного двійкового розряду випадкового числа, пристрій виконує перетворення аналогової величини амплітуди шумового сигналу та порівнює отримане дискретне значення з визначеним заздалегідь пороговим. Якщо значення більше порогового, то поточний біт випадкового числа приймається рівним 1, інакше – 0. Таким чином, для формування числа розрядністю n, потрібно виконати n таких операцій. Порогове значення визначається експериментально на етапі тестування пристрою.

Генерування істинно випадкових чисел потребує значного часу (за мірою комп'ютерної системи). У випадку генерації послідовності псевдовипадкових чисел, в якості початкового налаштування генератора може бути використане істинно випадкове число. В цьому випадку процес генерування наступних елементів послідовності відбувається на боці служби генерації. В системі реалізовано алгоритми генерування псевдовипадкових чисел BBS

(Blum-Blum-Shub) [1] та LFSR (Linear Feedback Shift Register) [2]. Система, що використовує апаратний генератор, працює в наступних режимах:

– генерування чергового істинно випадкового числа;

– початкове налаштування генератора за алгоритмом BBS;

– генерування чергового псевдовипадкового числа за алгоритмом BBS;

– початкове налаштування генератора за алгоритмом LFSR;

– генерування чергового псевдовипадкового числа за алгоритмом LFSR.

Проведено порівняльний аналіз якості наступних послідовностей чисел:

– дійсно випадкових чисел, отриманих за допомогою пристрою з джерелом лавинного шуму на основі стабілітрону (що розробляється в даній роботі);

– дійсно випадкових чисел, отриманих з атмосферного шуму за допомогою сервісу [3];

– послідовностей псевдовипадкових чисел, отриманих за алгоритмами BBS і LFSR з початковим налаштуванням дійсно випадковими числами за допомогою пристрою (що розробляється в даній роботі).

Ступінь випадковості послідовностей чисел оцінювалася за допомогою кейсу статистичних тестів NIST [4]. Для проведення тестування отримано чотири послідовності (по одній кожного типу, що вказані вище), які складаються з 20000 біт кожна. За результатами тестування видно, що всі відносно короткі послідовності мають хороші показники.

Також, для візуальної оцінки ступеню випадковості, було використано графічний тест, за допомогою якого можна спостерігати наявність (або відсутність) візуальних патернів в двійкових послідовностях. В даному випадку зображення складається з 141×141 пікселів. В результаті, на отриманих зображеннях істотних патернів не спостерігається. Таким чином, всі представлені послідовності випадкових чисел успішно проходять візуальний тест.

Висновки. Результати проведених тестів з набору NIST та візуальних тестів показали, що всі отримані послідовності чисел мають ознаки випадкових. Таким чином, в додатках з підвищеними вимогами до швидкодії, використання запропонованої системи в режимі генерування псевдовипадкових чисел (з дійсно випадковим налаштуванням) є виправданим. Однак зрозуміло, що для отримання більш повних результатів оцінки ступеню випадковості, варто оперувати послідовностями більшої довжини.

Інформаційні джерела

1. Blum L., Blum M., Shub M. A simple unpredictable pseudo-random number generator. SIAM Journal on Computing. 1986. Vol. 15, № 2. pp. 364–383.

2. Schneier B. Applied Cryptography. Protocols, Algorithms and Source Code in C. Wiley, 2017. 784 p.

3. Randomness and Integrity Services. URL: https://www.random.org

4. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / Rukhin A. and others. NIST Special Publication 800-22, Revision 1a, 2010. 131 p.

УДК 004.056

ІНТЕГРАЦІЯ КРИПТОГРАФІЇ ТА СТЕГАНОГРАФІЇ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ: АНАЛІЗ ПРОГРАМНИХ РІШЕНЬ

Ігор ГАЛИЦЬКИЙ
Тетяна ЛАВРИК
Сумський Державний Університет, м. Суми, Україна.

Abstract. *In a world where cyber threats are on the rise, new approaches to information security are needed. One of the effective methods is the integration of cryptography and steganography. This paper analyzes software solutions for crypto-stegographic systems, investigates their capabilities and limitations.*

Keywords: *cryptography, steganography, analysis, LSB method, crypto-steganographic system.*

Анотація. *У сучасному світі зростання кіберзагроз вимагає впровадження нових підходів для забезпечення безпеки інформації. Одним із ефективних методів є інтеграція криптографії та стеганографії. У цій роботі проведено аналіз програмних рішень для крипто-стеганографічних систем, досліджено їх можливості та обмеження.*

Ключові слова: *криптографія, стеганографія, аналіз, метод LSB, крипто-стеганографічна система.*

Крипто-стеганографічні системи є синергетичним поєднанням криптографічних і стеганографічних методів для забезпечення конфіденційності та захисту інформації. Криптографія перетворює дані у зашифровану форму, незрозумілу для сторонніх, тоді як стеганографія приховує їх у носіях, таких як зображення або аудіо. Такий підхід дозволяє створювати багаторівневий захист, де навіть у разі компрометації одного рівня інший залишається ефективним.

Процес інтеграції розпочинається із шифрування відкритого тексту за допомогою симетричних або асиметричних алгоритмів. Після цього зашифрований текст вбудовується у файл-носій за допомогою методів стеганографії. *Наприклад*, LSB-вставка дозволяє інтегрувати дані у найменш значущі біти пікселів зображення, що робить зміни практично непомітними для людського ока.

Основна перевага крипто-стеганографії полягає у забезпеченні одночасної таємності даних та їхньої непомітності. Це ідеальний інструмент для передачі конфіденційної інформації в умовах сучасних загроз, таких як перехоплення даних у відкритих мережах. Інтеграція цих двох методів дозволяє системам адаптуватися до різноманітних сценаріїв безпеки, зокрема для захисту корпоративних або особистих даних.

Різноманітний набір крипто-стегографічних систем, доступних сьогодні, спеціально розроблений для задоволення різних ситуацій і потреб безпеки, кожна з яких пропонує унікальні функціональні можливості та потенційні сфери застосування. Для аналізу було обрано чотири системи: OpenPuff, Steganos Security Suite, SilentEye і DeepSound. Вони демонструють різні підходи до інтеграції криптографії та стеганографії, а також орієнтовані на різні сценарії використання.

OpenPuff (рис. 1) підтримує широкий спектр форматів носіїв (зображення, аудіо, відео, документи) і забезпечує високий рівень безпеки завдяки багаторівневій архітектурі. Особливістю є метод непослідовного приховування, де зашифровані дані розподіляються між кількома файлами. Це ускладнює відновлення інформації навіть за умови часткової компрометації носія.

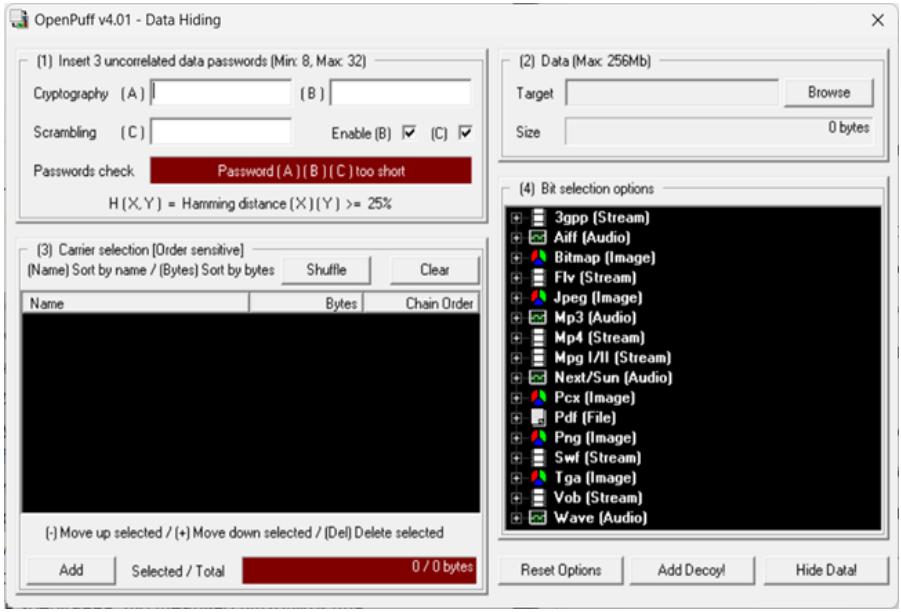


Рисунок 1 – Інтерфейс програми OpenPuff для приховування даних

Steganos Security Suite (рис. 2) пропонує комплексний підхід до захисту інформації, поєднуючи шифрування та стеганографію. Її ключові функції включають створення “віртуальних сейфів” для зберігання конфіденційних даних і знищення файлів за допомогою цифрового шредера. Окрім цього, Steganos дозволяє видаляти цифрові сліди, забезпечуючи конфіденційність користувача.

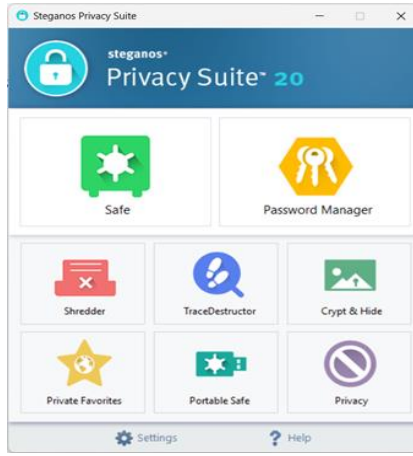


Рисунок 2 – Інтерфейс Steganos Security Suite з інструментами захисту

SilentEye (рис. 3) спеціалізується на базовій стеганографії з використанням LSB-методу для зображень і аудіофайлів. Інструмент має зручний інтерфейс і підходить для освітніх цілей або побутового використання, де не потрібен високий рівень безпеки. Проте, простота цього підходу створює вразливості до сучасних методів аналізу.

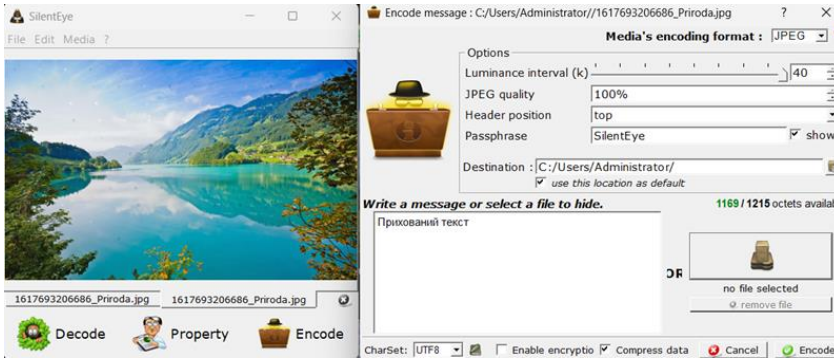


Рисунок 3 – Інтерфейс SilentEye для кодування повідомлень у зображення

DeepSound (рис. 4) спеціалізується на приховуванні даних у аудіофайлах із підтримкою форматів MP3 та WAV. Головна перевага – можливість захищати зашифровані дані без впливу на якість звуку. DeepSound підходить для завдань, де важлива непомітність інформації, але методи спектрального аналізу можуть становити загрозу.

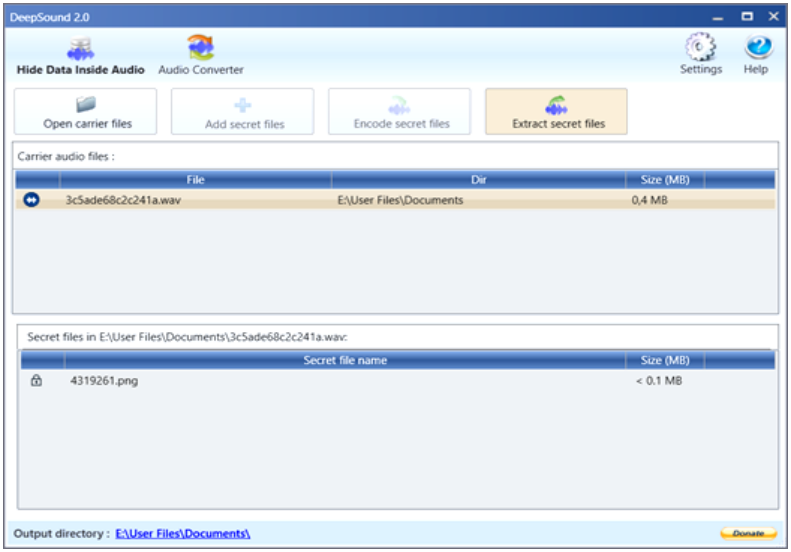


Рисунок 4 – Інтерфейс DeepSound для вбудовування файлів у аудіо

Проведений порівняльний аналіз вказаних вище стеганографічних і крипто-стеганографічних систем базувався на таких ключових аспектах, як підтримка форматів, методи шифрування, зручність користувача та специфічні випадки використання. У табл. 1 наведено результати проведеного аналізу.

Таблиця 1.

Порівняльний аналіз стеганографічних систем з функціями шифрування

Система	*Підтримувані формати*	*Методи шифрування*	*Зручність для користувача*	*Основний сценарій використання*
OpenPuff	JPEG, MP3, MP4, PDF, інші формати	Багатоалгоритмічне, багатошарове шифрування	Помірна	Вдосконалене приховування даних на різних носіях інформації
Steganos Security Suite	Широкий спектр, включаючи власні формати	256-бітний AES, двофакторна автентифікація	Висока	Повна конфіденційність із зашифрованими сейфами
SilentEye	JPEG, BMP, WAV, обмежена підтримка відео	AES-128, AES-256 (опціонально)	Висока	Базова стеганографія для освітніх цілей
DeepSound	MP3, WAV, FLAC	AES-256, додатковий захист парольною фразою	Помірна	Аудіо стеганографія з високим ступенем шифрування

Висновки. Аналіз продемонстрував, що вибір системи залежить від задач користувача: OpenPuff забезпечує високий рівень безпеки для корпоративного використання, тоді як SilentEye і DeepSound підходять для приватних потреб із меншими вимогами до захисту. Steganos Security Suite залишається універсальним інструментом для управління конфіденційною інформацією.

У подальшому планується розробити власну крипто-стеганографічна система, що буде спиратися на інтеграцію шифрування AES зі стеганографією LSB.

УДК [004.67/.021]:[004.056/.051]:004.421.5

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПРОСТИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ОБРОБКИ ЦИФРОВИХ ЗОБРАЖЕНЬ ІЗ ВИКОРИСТАННЯМ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Олег ГОРЯЧИЙ
Ігор ЖУРАВЕЛЬ
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *Steganographic methods of replacing the least significant bits (LSB) of digital images have several disadvantages that limit their application. A few simple modifications of these methods are proposed based on steganocontainer analysis and key size minimization using a pseudorandom sequence generator (PRSG). The efficiency of the proposed methods is analyzed in terms of detection resistance, throughput, key length, and algorithm performance.*

Keywords: *steganography, contrast, contours, coding, encryption, key.*

Анотація. *Стеганографічні методи заміни найменш значущих бітів (НЗБ) цифрових зображень мають ряд недоліків, що обмежують їх застосування. Запропоновано кілька простих модифікацій цих методів на основі аналізу стеганоконтейнера та мінімізації розміру ключа з використанням генератора псевдовипадкових послідовностей (ГПВП). Проаналізована ефективність запропонованих методів щодо стійкості до виявлення, пропускної здатності, довжини ключа та швидкодії алгоритмів.*

Ключові слова: *стеганографія, контраст, контури, кодування, шифрування, ключ.*

Вступ. Традиційні стеганографічні методи вбудовування даних в молодші розряди цифрових зображень (НЗБ) є все ще досить популярними, особливо в навчальних цілях, зважаючи на їх простоту та високу пропускну здатність таких стеганосистем [1–3]. Проте, такі стеганографічні методи вбудовування мають ряд суттєвих недоліків: низька стійкість до активних та пасивних атак, відсутність або значний розмір стеганоключа, високий ступінь помітності, легкість виявлення на основі статистичного аналізу чи з викори-

станням сучасних засобів стеганоаналізу [1, 4]. Інша проблема – захист цілісності та конфіденційності інформації у випадку, якщо факт вбудовування був виявлений [2, 5].

Мета і завдання дослідження. Метою роботи є розробка та порівняння простих модифікацій стеганографічних методів на основі заміни НЗБ на основі аналізу висококонтрастних та контурних ділянок стеганоконтейнера та використання ключів мінімального розміру на основі генератора псевдовипадкових послідовностей (ГПВП) [6]. Ефективність запропонованих методів будемо оцінювати на основі таких параметрів: стійкість до виявлення, пропускна здатність, довжина ключа та швидкодія.

Методи дослідження. Розглянемо базову модель стеганосистеми, що наведена на рисунку 1. Вбудовування інформації відбувається шляхом заміни одного або кількох НЗБ пікселів контейнера $C_v \in C$ бітами секретного повідомлення $M_i \in M$.

Рисунок 1 – Базова математична модель стеганосистеми

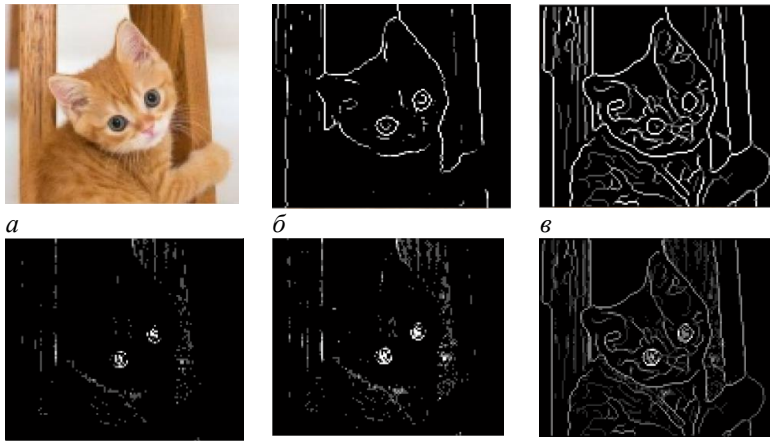
Перед вбудовуванням повідомлення може піддаватись процедурі попереднього кодування, *наприклад* архівації даних та завадостійкого кодування. З метою забезпечення непомітності, вбудовування доцільно виконувати у висококонтрастні, текстурні чи зашумлені ділянки зображення L [4], що отримуються блоком врахування особливостей контейнерів. Залежно від особливостей *L* та параметра порогового значення k_τ будемо динамічно змінювати кількість НЗБ I_τ для вбудовування в кожну з колірних компонент *R, G* та *B* контейнера $C_v^\tau, t = \overline{1,3}$. При цьому врахуємо, що людина більш чутлива до зміни яскравості зеленого кольору, ніж червоного, та найменш чутлива до синьої компоненти [1]. Оскільки людина частіше звертає увагу на передній план зображення, ми будемо виконувати обхід контейнера по

спіралі від країв зображення до його центру. Альтернативні методи вбудовування інформації – прямий обхід пікселів стеганоконтейнера чи випадковий їх вибір можуть спричинити візуальні зміни в контейнері.

Для визначення областей вбудовування будемо використовувати наступні формули:

$$L = \frac{1}{2}\left(L_e + L_c\right) = \frac{1}{6}\left(\sum_{t=1}^{3} \mathrm{Edge}\left(C_v^t, E_\alpha, e_\tau\right) + \sum_{t=1}^{3} \mathrm{Contrast}\left(C_v^t, C_\alpha, c_\tau\right)\right), \quad (1)$$

де L_e та L_c – нормалізовані оцінки контурних та контрастних пікселів контейнера C_v^τ (рис. 2). Аналіз контурів виконується методом Edge з використанням одного з стандартних алгоритмів виявлення E_α, *наприклад* Кенні чи Собеля, та порогу e_τ. Для обчислення контрасту використовується метод $\mathrm{Contrast}$ на основі формули Міхельсона C_α для кожного пікселя C_{ij} та середньої інтенсивності значень $\overline{L}_{ij}$ в блоці сусідніх елементів цього пікселя розміру 3×3 та порогового значення контрасту c_τ.



а *б* *в*

г *д* *е*

Рисунок 2 – Аналіз вхідного контейнера C_v: *а* – зображення “cat.jpg” (128×108 пікс. 14 КБ) *б, в* – визначення контурів L_e алгоритмами Собеля та Кенні; *г, д* – визначення контрасту L_c при $c_\tau = 0,2$ та $c_\tau = 0,15$; *е* – загальна оцінка L для алгоритму Кенні та $c_\tau = 0,15$.

Коротка характеристика запропонованих методів. У методах 1, 2а, 2б (аналіз контурних L_e та контрастних ділянок L_c контейнера, фіксоване чи динамічне кодування, стиснення ключа з використанням кодів Гаффмана) ключова послідовність формується під час вбудовування даних. У методах

3а–3в (стеганонезалежний аналіз контурних L_e та контрастних ділянок L_c модифікованого контейнера, фіксований розмір ключа) перед визначенням областей вбудовування L певним чином модифікується вхідний контейнер C_v^τ, *наприклад* з використанням бітової маски K_v^τ на основі ГПВП. (рис. 3). Додатково можемо застосовувати шифрування даних методом одноразового блокноту (метод 3в). В цій роботі як для побудови маски K_v^τ стеганоконтейнера, так і для формування криптографічного ключа K_e будемо використовувати швидкі генератори із [6] на основі апроксимації функції $y = 1/\sqrt{x}$ в арифметиці з рухомою комою, *наприклад* rsqrt2dc_everyBit (1/0). Для спрощення програмної реалізації залежно від 64-розрядного початкового значення x_0 ГПВП псевдовипадкову послідовність будемо зчитувати з відповідного бінарного файлу.

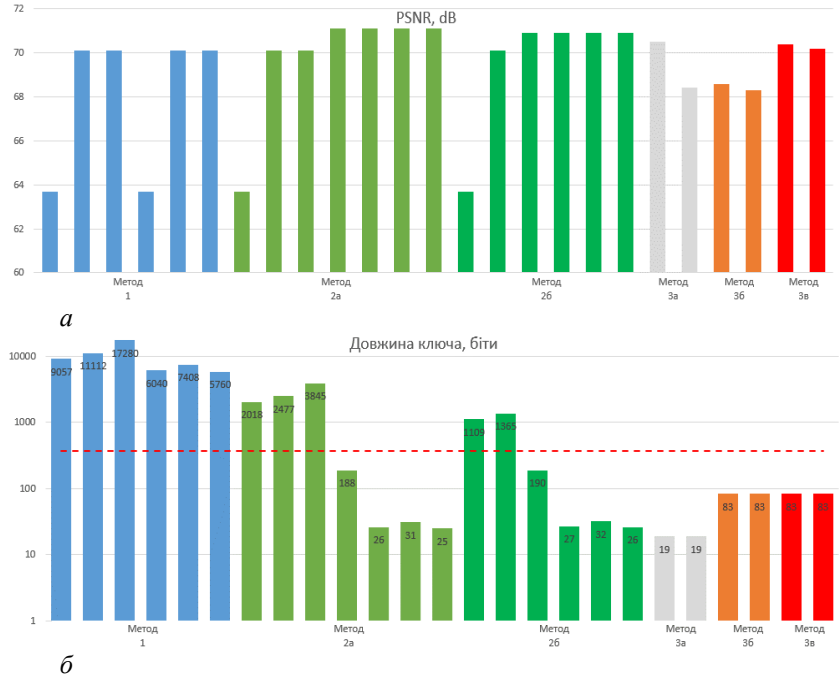


Рисунок 3 – Порівняння ефективності різних стеганографічних методів для C_v “cat.jpg” (алгоритм Кенні, $c_\tau = 0{,}15, k_\tau = 0{,}5$, різні значення I_τ) у випадку 368-бітного повідомлення M_i: *а* – похибки вбудованого контейнера S_v за піковим співвідношенням сигналу до шуму; *б* – реальні довжини стеганоключа K_i.

Одержані результати. Для обраного прикладу C_v було досліджено різні варіанти реалізації запропонованих методів, зокрема щодо кількості вбудованих НЗБ I_τ в залежності від L та порогового значення k_τ, формування ключової послідовності K_l, її кодування та механізмів стиснення. Ефективність розглянутих стеганографічних алгоритмів аналізувалась, зокрема, на основі наступних параметрів: стійкість до виявлення (візуальна якість, максимальна різниця, середньоквадратична похибка (RMSE), пікове співвідношення сигналу до шуму (PSNR)); пропускна здатність (максимальна довжина повідомлення); довжина ключа (мінімальна довжина K_l та коефіцієнт стиску); кількість згенерованих псевдовипадкових біт та швидкодія алгоритму в середовищі Matlab. У випадку 368-бітного повідомлення M_i основні результати наведені на рисунку 3.

Висновки. Було запропоновано декілька простих модифікацій стеганографічних методів на основі заміни НЗБ, що виконують аналіз висококонтрастних та контурних ділянок стеганоконтейнера та використовують ключі мінімального розміру на основі ГПВП. Було проведено аналіз та порівняння запропонованих методів за основними показниками. Ці методи дозволяють динамічно регулювати помітність модифікації стеганоконтейнера та обсяг вбудованих даних, максимально зменшити розмір стеганоключа при достатньому рівні захисту вбудованих даних.

Інформаційні джерела

1. Ковтун В., Гнатюк С., Кінзерявий О. Систематизація сучасних методів комп'ютерної стеганографії. Безпека інформації. 2013. Т. 19, № 3. – С. 209–217.

2. Кузнецов О. О., Євсеєв С. П., Король О. Г. Стеганографія : навч. посіб. Харків : ХНЕУ, 2011. 232 с.

3. Бекіров А., Ященок В., Крейдун О. Стеганографічний метод на основі безпосереднього та непрямого вбудовування даних для областей зображення з різною насиченістю. Сучасні інформаційні технології у сфері безпеки та оборони. 2019. Т. 34, № 1. – С. 115–120.

4. Image disentanglement autoencoder for steganography without embedding / X. Liu et al. 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) : conf., New Orleans, LA, USA, 18–24 June 2022. 2022. pp. 2293–2302.

5. Rani S., Kurniawardhani A., Rendani Y. A. W. Steganography on digital color image using modulo function and pseudo-random number generator. International Journal on Advanced Science, Engineering and Information Technology. 2021. Vol. 11, no. 6. pp. 2470–2475.

6. Горячий О., Максимович В., Шабатура М. Дослідження множини початкових значень генераторів псевдовипадкових чисел на основі арифметики з рухомою комою. Сучасний захист інформації. 2024. Т. 58, № 2. – С. 91–102.

УДК 004.932:004.056.55

СТАН ДОСЛІДЖЕНЬ У СФЕРІ ЦИФРОВОГО МАРКУВАННЯ ДЛЯ АУДІОФАЙЛІВ

Остап-Святосла МАЛЕЦЬ
Ольга СМОТР
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The paper aims to study the current state of the art in the field of digital audio content marking and to outline promising areas of research in the field of digital audio content watermarking. To achieve this goal, the paper uses a systematic review and analysis of scientific articles on the practical implementation of existing digital watermarking methods, a method of comparing results, and a method of synthesizing results. Based on the conducted research, a comprehensive picture of the current state of digital audio content labeling was obtained, the relevance of the research topic was proved, and promising areas of application of these technologies were identified.*

Keywords*: digital watermark, audio content, security, information technology, digital watermarking technologies, neural network.*

Анотація*. У роботі проведено дослідження сучасного стану у сфері цифрового маркування аудіоконтенту та окреслити перспективні напрямки досліджень в галузі цифрового водяного маркування аудіоконтенту. Для досягнення поставленої мети в роботі використано систематичний огляд та аналіз наукових статей, щодо практичних реалізацій існуючих методів цифрового водяного маркування, метод порівняння результатів та метод синтезу результатів. Базуючись на проведених дослідженнях, отримано комплексне уявлення про сучасний стан маркування цифрового аудіоконтенту, доведено актуальність теми дослідження та виділено перспективні напрямки застосування цих технологій.*

Ключові слова*: цифровий водяний знак, аудіоконтент, безпека, інформаційні технології, технології цифрових водяних знаків, нейронна мережа.*

Цифровізація суттєво спростила створення, розповсюдження та обмін аудіоконтентом. Однак із зростанням доступності цифрових медіа почастішали випадки несанкціонованого копіювання та поширення аудіофайлів, що порушують права інтелектуальної власності. Це створює значні виклики для власників контенту, які прагнуть захистити свої твори від піратства та отримувати справедливу винагороду за їх використання.

Для захисту аудіоконтенту сьогодні застосовують різні методи, такі як шифрування файлів, управління цифровими правами (DRM), технології цифрових водяних знаків і методи аутентифікації. Серед них цифрові водяні знаки мають унікальні переваги, зокрема здатність відстежувати контент і

визначати його походження. Ці технології дають змогу ідентифікувати власника та захищати контент навіть після подальшого розповсюдження.

Водночас існують низка невирішених проблем, серед яких забезпечення стійкості водяних знаків до різних видів аудіообробки, таких як стиснення, зміна швидкості відтворення або додавання шуму. Важливим залишається завдання зробити водяні знаки непомітними для слухачів, зберігаючи якість звуку, що є особливо актуальним у сучасних потокових сервісах. Удосконалення надійних і універсальних методів захисту контенту залишається пріоритетним напрямом для наукових досліджень і розробок.

Сучасний розвиток алгоритмів штучного інтелекту та їх доступність сприяли активному використанню нейронних мереж у системах водяного маркування аудіоконтенту [1–6]. *Наприклад*, у дослідженні Pengcheng Li, Xulong Zhang, Jing Xiao та Jianzong Wang [1] представлено модель подвійного вбудовування водяних знаків, яка покращує ефективність маркування та підвищує стійкість до атак, аналізуючи вплив рівня атак на інвертовану нейронну мережу під час навчання. Однак, як і раніше, залишається актуальним питання забезпечення стійкості до нових типів атак без втрати якості звуку. Інше дослідження [2] пропонує використання глибокої нейронної мережі та перцептивних втрат для вбудовування водяних знаків із врахуванням психоакустичних ефектів.

У роботі [3] наведено огляд сучасних методів водяного маркування з використанням глибоких нейронних мереж, включно з новою таксономією. Водночас автори наголошують на відсутності єдиної методології для оцінки ефективності таких методів, що підкреслює необхідність стандартизації.

Дослідження [4] розглядає застосування згорткових нейронних мереж для підвищення стійкості до атак, а в роботі [5] представлено метод навчання на основі контрзаходів. Втім, ці методи не завжди є ефективними для нових і непередбачуваних атак.

Узагальнену схему системи, що поєднує глибоке навчання з підходом до нанесення водяних знаків на аудіо наведено на рисунку 1. Окреслено основні компоненти системи, включаючи вилучення ознак, класифікацію за допомогою глибоких нейронних мереж (DNN) та процес нанесення водяних знаків.

Запропонована система вбудовує водяний знак за допомогою методу DCT-MLP-LSB, призначеного для характеризації та класифікації аудіо за такими категоріями, як музика, мова, стать та емоції. Експериментальні результати демонструють ефективність системи як на відкритих наборах даних, так і стійкість водяних знаків. Для додатків, що не пов’язані з безпекою, стійкість до навмисних атак не є критичною, але стійкість до обробки сигналу, *наприклад*, стиснення, є необхідною. У цьому випадку водяний знак містить метадані, такі як інформація про виконавця або місце реєстрації, що допомагає індексувати сигнал.

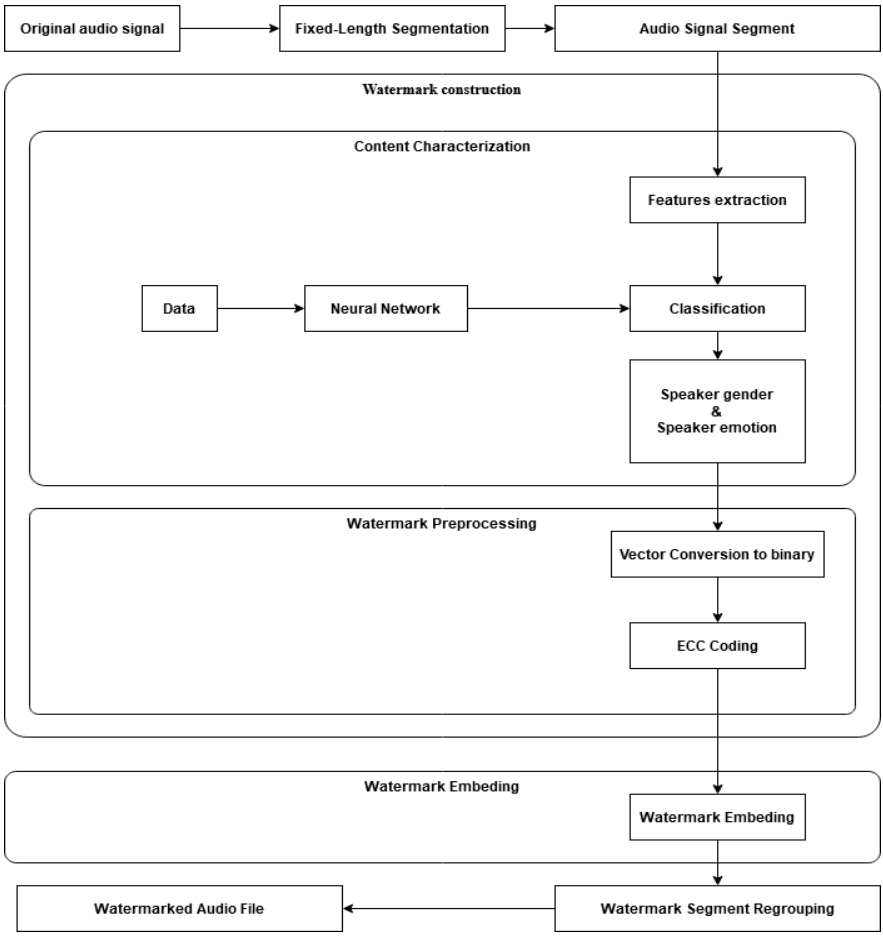


Рисунок 1 – Узагальнена схема нанесення водяних маркерів на аудіоконтент

Висновки. Попри значний прогрес у використанні нейронних мереж для водяного маркування аудіоконтенту, залишається багато питань для подальших досліджень, зокрема забезпечення стійкості до атак, оптимізація якості звуку та створення єдиних стандартів оцінки ефективності методів.

Інформаційні джерела

1. Charfeddine M., Mezghani E., Masmoudi S., Amar C. B. and Alhumyani H. “Audio Watermarking for Security and Non-Security Applications”, in IEEE Access, vol. 10, pp. 12654–12677, 2022. doi: 10.1109/ACCESS.2022.3145950.

2. Zhou J. and Chen P. “Generalized Discrete Cosine Transform”, 2009 Pacific-Asia Conference on Circuits, Communications and Systems, Chengdu, China, 2009, pp. 449–452. doi: 10.1109/PACCS.2009.62.

3. Kurdi M. M., Elzein I. A. and Zeki A. M., “Least Significant Bit (LSB) and Random Right Circular Shift (RRCF) in digital watermarking”, 2016 12th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 2016, pp. 111–116. doi: 10.1109/ICENCO.2016.7856454.

4. Gupta A., & Yilmaz A. (2018). Social network inference in videos. In Elsevier eBooks, pp. 395–424.

5. Ramirez A. D. P., de la Rosa Vargas J. I., Valdez R. R. and Becerra A., “A comparative between Mel Frequency Cepstral Coefficients (MFCC) and Inverse Mel Frequency Cepstral Coefficients (IMFCC) features for an Automatic Bird Species Recognition System”, 2018 IEEE Latin American Conference on Computational Intelligence (LA-CCI), Gudalajara, Mexico, 2018, pp. 1–4. doi: 10.1109/LA-CCI.2018.8625230.

6. Martyn Y., Smotr O., Burak N., Prydatko N. and Malets I., Informational graphic technologies for fire safety level determination in special purpose buildings, in: Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020, 2020, pp. 398–403. doi: 10.1109/DSMP47368.2020.9204180.

УДК 004.421.5:511

АНАЛІЗ ЕФЕКТИВНОСТІ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ КВАДРАТНОГО КОРЕНЯ ПРОСТОГО ЧИСЛА

Олег ГОРЯЧИЙ
Захар ЯРЕМЧУК
Національний університет “Львівська політехніка”, м. Львів, Україна.

Abstract. *This paper explores the use of irrational numbers obtained by calculating the square root of primes for pseudorandom number generators. The goal is to evaluate their effectiveness in terms of generation speed and statistical characteristics by the NIST STS standard. Algorithms and verification methods are developed.*

Keywords: *irrational numbers, square root, PRNG, NIST STS, prime numbers.*

Анотація. *У цій роботі досліджується використання ірраціональних чисел, отриманих через обчислення квадратного кореня простих чисел, для генераторів псевдовипадкових послідовностей. Мета – оцінити їх ефективність за швидкістю генерації та статистичними характеристиками відповідно до стандарту NIST STS. Розроблено алгоритми та методи перевірки.*

Ключові слова: *ірраціональні числа, квадратний корінь, ГПВЧ, NIST STS, прості числа.*

Псевдовипадкові числа (ПВЧ) відіграють ключову роль у багатьох галузях, зокрема в криптографії, комп'ютерній графіці, чисельних симуляціях та статистичному моделюванні. Оскільки ірраціональні числа мають нескінченну нерегулярну послідовність цифр, вони привертають увагу як потенційне джерело ПВЧ [1, 2]. Особливий інтерес викликають квадратні корені $Y = \sqrt{P}$ простих чисел P, які мають математично доведену ірраціональність і складну структуру. В даній роботі було протестовано та порівняно деякі методи обчислення квадратних коренів за швидкодією. Потім згенеровано послідовності цифр обчислених коренів від простих чисел та досліджено їх статистичні властивості за допомогою набору тестів NIST Statistical Test Suite [1].

1. Аналіз методів генерації

Для оцінки ефективності методів обчислення квадратного кореня довільної точності проведено тестування для простого числа $P = 294131$ із наступними рівнями точності: 10 000, 100 000, 1 000 000 і 10 000 000 бітів. Для тестування використовувались три основні методи: "цифра за цифрою" [2, 3], метод Галлея з динамічною точністю [4] та ітеративний метод із двома змінними [3].

Результати показують, що вибір методу залежить від цілей задачі. Метод "цифра за цифрою" є доцільним для задач із низькими вимогами до швидкості та високими вимогами до точності. Метод Галлея з динамічною точністю є ітеративним підходом, що використовує розширену формулу Ньютона для швидкої збіжності та динамічну адаптацію точності, забезпечуючи високу продуктивність навіть при великих обсягах обчислень [4]. Ітеративний метод з двома змінними, що має квадратичну збіжність, може бути корисним у вузькоспеціалізованих задачах, де ключовою є стійкість до похибок, а час виконання не є критичним. Результати досліджень наведені в таблиці 1.

Таблиця 1

Результати швидкодії методів обчислення квадратного кореня

Метод	*Довжина згенерованої послідовності*			
	10 000 біт	*100 000 біт*	*1 000 000 біт*	*10 000 000 біт*
"Цифра за цифрою"	0,004 с	0,25 с	25 с	4 800 с
Метод Галлея	0,008 с	0,45 с	4 с	90 с
Ітеративний метод із двома змінними	0,045 с	4,4 с	830 с	660 514 с

Отже, для подальших досліджень було обрано метод Галлея кубічної збіжності. Цей метод став оптимальним рішенням для генерації ПВЧ, поєднуючи швидкість і точність.

2. Оцінка статистичних властивостей коренів квадратних простого числа

Для проведення дослідження було згенеровано 100 послідовностей довжиною 10^8 біт кожна, які були обчислені як корені від 100 різних простих чисел, обраних випадково. Результати тестування наведено на рисунку 1.

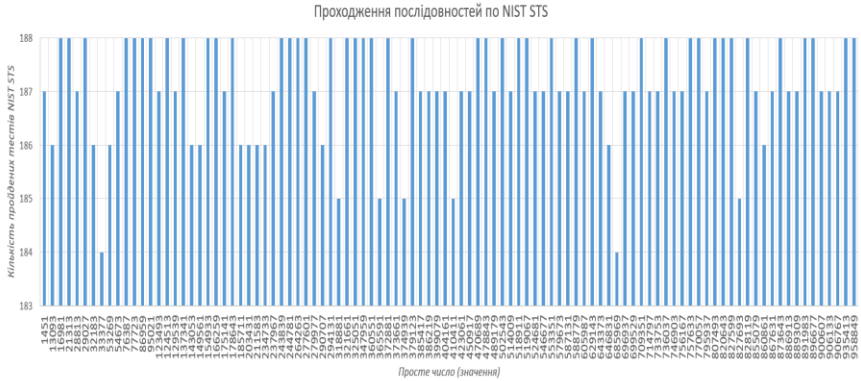


Рисунок 1 – Гістограма результатів проходження послідовностей по NIST STS

Для оцінки якості згенерованих послідовностей було використано статистичний пакет NIST Statistical Test Suite, який містить 15 груп тестів для перевірки випадковості. Результати показали, що послідовності, згенеровані на основі квадратних коренів, проходять у середньому лише 186 з 188 тестів, що не відповідає високим стандартам для криптографічних застосувань.

3. Метод конкатенації послідовностей

Через повільність генерації ПВЧ, можливі статистичні недоліки та потенційну вразливість до операції реверсного аналізу, де можна отримати вхідне значення P, з якого було згенеровано послідовність (а де-факто початкове значення для ПВЧ), було запропоновано метод конкатенації послідовновностей ПВЧ. Цей метод поєднує декілька послідовностей з квадратних коренів простих чисел меншої точності та довжини. Було сформовано 10 послідовностей довжиною 10^9 біт, з яких обрано $m = 10$, 100 та 1000 тестових фрагментів довжиною 10^6 біт. Усі фрагменти пройшли перевірку NIST STS із високими результатами, за винятком єдиного провалу тесту на збіги шаблонів, що не перекриваються (Non-Overlapping Template Test). Одержані результати тестування наведені в таблиці 2. Як бачимо, єдиний тест, що дав негативний результат для послідовності № 7, стосувався Non-Overlapping Template Test, у якому з 148 використаних підтестів не був пройдений лише один. Це свідчить про мінімальні нерегулярності, які не впливають суттєво на загальну випадковість послідовностей.

Таблиця 2

Результати статистичного тестування конкатенованих послідовностей ПВЧ

Номер	*Конкатенація послідовностей ПВЧ з коренів квадратних від набору простих чисел*	*Провалені тести NIST STS*		
		m=10	*m=100*	*m=1000*
1.	277601, 32183, 372881, 290707, 29027, 404161, 579673, 373661, 321661, 211583	0	0	0
2.	325051, 175141, 185711, 714797, 137341, 365591, 478843, 518911, 906767, 828119	0	0	0
3.	347959, 386219, 736037, 399079, 891983, 733753, 243839, 646831, 294131, 886913	0	0	0
4.	450917, 588779, 807493, 143053, 906133, 423061, 234733, 379123, 827693, 709351	0	0	0
5.	470689, 757633, 696937, 958849, 502543, 178643, 264263, 77723, 95021, 896677	0	0	0
6.	519067, 203431, 86959, 154933, 123493, 873643, 385417, 279977, 935413, 820643	0	0	0
7.	76387, 33377, 524681, 587131, 489179, 643373, 374939, 318881, 889309, 28813	0	0	1
8.	827599, 1451, 360551, 553351, 54673, 546677, 514009, 410411, 685969, 166259	0	0	0
9.	860861, 21313, 13093, 129539, 605987, 770057, 53269, 149561, 699529, 16981	0	0	0
10.	900607, 756167, 629143, 795937, 855079, 867631, 746903, 124513, 237967, 244781	0	0	0

Висновки. Як було показано в роботі, квадратні корені простих чисел потенційно можуть бути використані для генерації ПВЧ, що відповідають статистичним вимогам щодо випадковості [1]. Запропонований метод конкатенації дозволяє суттєво покращити швидкість генерації, статистичні характеристики та криптографічну стійкість сформованих послідовностей. Провал деяких статистичних тестів може свідчити про мінімальні нерегулярності, які суттєво не впливають на практичне використання. Подальші дослідження будуть спрямовані на аналіз впливу параметрів генерації ПВЧ та розширене тестування з використанням інших статистичних пакетів, зокрема Diehard та TestU01.

Інформаційні джерела

1. Rukhin A., et al. (2010). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication.

2. Горпенюк А., Лужецька Н. Генератор псевдовипадкових чисел на обчислювачі кореня квадратного з простого числа. Вісник НУ Львівська політехніка “Автоматика, вимірювання та керування”. 2013, № 753. – С. 45–50.

3. Methods of computing square roots. Wikipedia. URL: https://en.wikipedia.org/wiki/ Methods_ of_ computing_square_roots (дата звернення: 20.11.2024).

4. Vestermark H. Fast Square Root and inverse calculation for Arbitrary Precision number. 2023. 29 p.

Напрям 7

КІБЕРБЕЗПЕКА ІНФРАСТРУКТУРИ

UDC 004.056.53: 004.942

HARDWARE-SOFTWARE APPROACH TO ENSURING INFORMATION SECURITY IN AUTOMATED METROLOGICAL CONTROL SYSTEMS FOR PRODUCTION PROCESSES

***Ulyana PANOVYK*[1,2]**
***Roman HIDEY*[2]**

[1]***Department of Information Security Management, Lviv State University of Life Safety, Lviv, Ukraine.***

[2]***Department of Computer Technologies in Publishing and Printing Processes, Lviv Polytechnic National University, Lviv, Ukraine.***

Анотація. *Розроблено апаратно-програмний комплекс, що поєднує апаратні та програмні засоби для створення комплексної системи захисту даних. Виконано оцінку ефективності рішення, включаючи захищеність даних, швидкість обробки та стійкість до загроз. Результати показали, що апаратно-програмний підхід перевершує традиційні методи за всіма ключовими показниками, забезпечуючи вищий рівень безпеки, продуктивності та надійності.*

Ключові слова: *апаратно-програмний комплекс, інформаційна безпека, автоматизовані системи, виробничі процеси, ефективність системи, стійкість до атак.*

Abstract. *A hardware-software complex has been developed, combining hardware and software tools to create an integrated data protection system. An assessment of the solution's effectiveness was conducted, covering data security, processing speed, and resilience to threats. The results demonstrated that the hardware-software approach outperforms traditional methods in all key metrics, providing higher levels of security, performance, and reliability.*

Keywords: *hardware-software complex, information security, automated systems, production processes, system efficiency, resilience to attacks.*

Information security is a key aspect of modern automated production processes, especially in metrological systems that ensure the accuracy and reliability of quality control. Automated metrological systems process a large volume of sensitive data on production parameters, which requires protection from unauthorized access, manipulation, and failures. Amid growing cyber threats, ensuring reliable information security in these systems is critically

important to maintaining the stability and quality of production processes. The main threats to information security in automated metrological systems include unauthorized access, which can lead to data manipulation or loss; cyber threats, such as viruses and malware, that can disrupt system operation; and hardware failures, which affect measurement accuracy and can result in losses [1].

Ensuring robust information security in metrological systems requires both hardware and software solutions to protect data, measurement accuracy, and system reliability. Key protection methods include:

– data encryption at the transmission and storage levels using AES and RSA algorithms to prevent unauthorized access;

– authentication and access control with methods like multi-factor authentication, biometrics, and protocols such as LDAP and OAuth to restrict access to critical areas;

– real-time monitoring to detect and respond quickly to anomalies, reducing cyber incident risks with tools like SIEM systems [2].

Traditional security approaches are often ineffective in production environments due to the complexity of metrological systems with numerous hardware and software components. Key limitations include data processing delays from real-time encryption, vulnerability to physical attacks, and challenges in integrating diverse, potentially incompatible security systems, which increase vulnerability risks. These limitations underscore the need for comprehensive hardware-software solutions tailored to production environment requirements for adequate protection.

The hardware-software complex (HSC) for data protection in metrological systems combines hardware components (sensors, controllers, secure network interfaces) with specialized software that provides data security control, monitoring, and analysis. The main components of the HSC include:

– data collection and transmission system – hardware sensors and data collection devices that gather information from various production processes;

– data processing controllers – perform initial data processing and filtering, ensuring reliability and accuracy before transmitting information to the main server;

– secure storage server – a central storage location where data encryption and protection against unauthorized access are implemented;

– monitoring software interfaces – provide user access to information and real-time management of security parameters.

The HSC software performs data collection and processing, system status monitoring, as well as filtering and alerting for potential threats. With integrated encryption and multi-level authentication, it minimizes the risk of data compromise. Key functions include data encryption during transmission and storage to protect confidentiality, anomaly detection based on behavioral analysis and machine learning algorithms, and automatic security module updates to respond to new threats.

The architecture of the hardware-software complex requires attention to physical security measures that ensure resilience against tampering and unauthorized access. In modern automated metrological systems, encryption plays a key role in protecting data confidentiality and integrity, particularly through symmetric and asymmetric algorithms. For example, AES (Advanced Encryption Standard) allows fast encryption of large data volumes, which is essential for real-time streaming data, while RSA is used for secure encryption key protection as a reliable asymmetric encryption method. Access management employs various models, such as Role-Based Access Control (RBAC), providing flexibility in configuring access rights according to user roles, thus reducing the risk of unauthorized access. Enhanced security is achieved through authentication and authorization protocols that verify user legitimacy and control access to resources. For instance, the OAuth 2.0 protocol provides limited access to users and applications without sharing credentials, while LDAP (Lightweight Directory Access Protocol) is used for centralized access management and authentication [3].

After examining individual hardware and software security methods, the need arises to create a unified, comprehensive system that integrates all security measures for maximum effectiveness. Integrating hardware and software solutions is a crucial step toward a comprehensive security system that ensures reliable information security in metrological systems. This integration process includes synchronizing the operation of hardware and software components for effective real-time data monitoring, control, and protection. During integration, hardware components such as cryptographic modules and controllers are combined with software tools for authentication, encryption, and access control, enabling the hardware-software complex to quickly detect threats and respond to risks, thereby reducing the likelihood of unauthorized access to sensitive information [4].

To ensure the integration of hardware and software components, models are used to describe the interaction of components within the system. One such model is the multi-layered security model, which consists of several levels: the physical security layer, the access control layer, and the data protection layer. Each layer provides both hardware and software protection, enhancing the system's resilience to threats (Fig. 1).

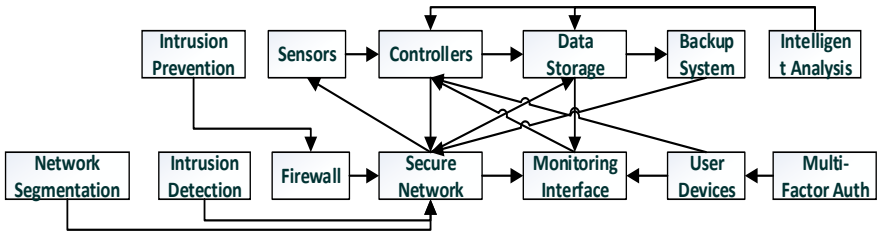


Figure 1 – Operating Algorithm of the Hardware-Software Complex

The process of the hardware-software complex involves the interaction of components for data collection, processing, storage, monitoring, and protection in a production environment. Sensors collect information and transmit it to controllers, which process the data for further storage on data storage servers in encrypted form. The monitoring interface provides real-time access to data, while a secure network and firewall ensure transmission security and prevent unauthorized access. The backup system creates data backups, and user devices use multi-factor authentication for enhanced access security. Intrusion detection and prevention systems protect against threats, while intelligent data analysis systems detect anomalies. Network segmentation mechanisms limit the spread of threats, ensuring reliable data protection.

To evaluate the effectiveness of the proposed hardware-software complex in comparison with traditional methods, various criteria are applied. The main indicators include:

1. Data security – the level of data protection from unauthorized access, measured by the security coefficient $C_S : C_S = D_p / D_t$, where D_p is the volume of protected data, and D_t is the total volume of processed data. The closer C_S is to 1, the higher the level of data security.

2. Processing speed – the time required to process data, which affects system performance in real conditions: $T_0 = 1/R$, where T_0 is the average processing time per request, and R is the number of requests processed per second. A lower T_0 value indicates higher performance.

3. Resilience to attacks – the system's ability to withstand external and internal threats, determined by the resilience of components to various types of attacks: $S_0 = \sum W_i \times R_i$, where W_i is the weight of security against a specific type of attack, and R_i is the level of resilience to the corresponding threat.

In the course of the study, the effectiveness of the proposed hardware-software approach was compared with traditional information protection methods in automated metrological systems. The proposed solution was tested in real production conditions, where its level of security, performance, and resilience to attacks were evaluated.

The hardware-software approach demonstrated significant advantages over traditional protection methods. The level of data security increased from 0.75 to 0.95, indicating a 25% improvement. Data processing speed improved from 150 ms to 90 ms, making it 40% faster and enabling efficient real-time monitoring. Resilience to attacks also increased from 7 to 9 points, showing higher reliability of the proposed system compared to traditional approaches. Thus, the proposed hardware-software complex significantly outperforms traditional methods in terms of security, processing speed, and attack resilience, confirming its effectiveness and suitability for implementation in automated metrological systems.

Conclusions. To further enhance the hardware-software complex for information security, it is recommended to expand encryption algorithms for greater data protection flexibility and resilience to new threats. Integrating machine learning for anomaly detection enables rapid response to security threats, while improved monitoring and analytics ensure detailed system control and timely vulnerability detection. The proposed approach is effective for information security in metrological systems, and ongoing research will further boost its effectiveness in dynamic production environments.

Information sources

1. Panovyk U., Hidei R., Bohonis O. (2024). Integrated metrology systems in Industry 4.0. Scientific Papers, № 1(68). pp. 71–82. URL: https://doi.org/10.32403/1998-6912-2024-1-68-71-82.

2. Bhosale P., Kastner W. & Sauter T. (2022). Automating Safety and Security Risk Assessment in Industrial Control Systems: Challenges and Constraints. IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–4. doi: 10.1109/ETFA52439.2022.9921517.

3. Wang Y. et al. (2019). Reliability Assessment Model for Industrial Control System Based on Belief Rule Base. International Journal of Computers Communications & Control. 2019. Vol. 14, no. 3. pp. 419–436. URL: https://doi.org/10.15837/ijccc.2019. 3.3548

4. Wai Eric C. H. & Lee C. (2024). Depth in Defense: A Multi-layered Approach to Cybersecurity for SCADA Systems in Industry 4.0. Science and Technology: Recent Updates and Future Prospects, Vol. 2. pp. 124–144. doi: 10.9734/bpi/strufp/v2/12542F.

UDC 004.056.5:004.738.5

SECURE ACCESS TO ENTERPRISE INFORMATION SYSTEMS IN THE MODERN DIGITAL ENVIRONMENT

Ulyana PANOVYK [1, 2]
Serhii KUTAS [2]
Amina QURESHI [3]

[1]***Department of Information Security Management, Lviv State University of Life Safety, Lviv, Ukraine.***

[2]***Department of Computer Technologies in Publishing and Printing Processes, Lviv Polytechnic National University, Lviv, Ukraine.***

[3]***Security and access management specialist in Nestle, United Kingdom and Ireland.***

Анотація. *Розглядаються основні аспекти безпечного доступу до інформаційних систем підприємств, включаючи управління обліковими записами, політику паролів, розподіл обов'язків, контроль сенситивної інформації та аудит. Окремо висвітлено управління ризиками і підвищення обізнаності співробітників. Подано рекомендації для вдосконалення політики доступу і перспективи застосування новіт-*

ніх технологій, як-от багатофакторна автентифікація та штучний інтелект, для підвищення рівня безпеки.

Ключові слова: *безпека доступу, управління ризиками, політика паролів, контроль доступу, сенситивна інформація, аудит.*

Abstract. *The key aspects of secure access to enterprise information systems are considered, including account management, password policies, role segregation, sensitive information control, and auditing. Risk management and employee awareness enhancement are highlighted. Recommendations are provided for improving access policies and exploring the potential of new technologies, such as multi-factor authentication and artificial intelligence, to enhance security levels.*

Keywords: *access security, risk management, password policy, access control, sensitive information, audit.*

In the modern digital environment, secure access to enterprise information systems is crucial. Technologies like cloud computing, IoT, and AI have increased the data volume on corporate platforms, but many enterprises remain vulnerable due to insufficiently protected access systems, posing risks of significant financial and reputational loss. Key challenges include human risks (e.g., simple passwords and phishing), a 40% rise in cybercrime over five years–especially ransomware attacks–and the complexity of access management in multi-component systems, which creates exploitable vulnerabilities. Thus, secure access requires a comprehensive approach to address modern threats [1].

The foundation of access control to information systems is account management, as user accounts define identity, permissions, and restrictions. For example, individual accounts in systems like Microsoft Active Directory or Okta allow tracking of each employee's activity, which is crucial for security, especially with a large number of users. Account management policies should minimize compromise risks by enforcing unique accounts, least privilege, regular permissions updates, and automated administration. The principle of uniqueness provides personal accounts, facilitating audits, while the least privilege principle restricts user access to necessary resources, reducing unauthorized access risks. For instance, in a Role-Based Access Control (RBAC) system like Cisco Identity Services Engine (ISE), access rights can be configured according to the employee's role. Regular permissions updates involve reviewing access when job roles change, and automated management through tools like CyberArk or Thycotic enhances efficiency and reduces error likelihood. Upon termination, employee accounts should be closed or access modified in systems to prevent data misuse.

In corporate environments, passwords are a common authentication method, but their security limitations can be risky. An effective password management policy includes a minimum password length (at least 12 characters with uppercase, lowercase, numbers, and symbols), regular updates every 90

days, prevention of reuse, and protection through hashing and encryption. Additional security is provided by two-factor authentication (2FA), such as Google Authenticator or Microsoft Authenticator, which requires both a password and a one-time code, reducing the risk of compromise during phishing attacks. Password management tools like LastPass or Keeper generate strong passwords, store them securely, and audit password activity. Automated solutions enhance security and simplify administration, making them a crucial element of security policy [2].

Password and authentication policies provide basic account and access protection. An essential next step is role segregation and the principle of least privilege. While password policies ensure authentication reliability, role segregation and access restrictions control who can access data, reducing the risks of internal threats and conflicts of interest. The principle of least privilege grants employees only the rights necessary for their roles, enhancing security. For example, a marketing employee does not have access to financial resources if it is not part of their job responsibilities.

Role segregation helps avoid conflicts of interest and reduces internal threats by distributing key functions among employees. For instance, in systems like Microsoft Active Directory or Okta, an employee with access to financial data does not have permission to manage access, ensuring control. Access rights distribution is based on clear role differentiation: the system administrator has full access for system configuration and management, finance department employees have limited access to financial information, and the marketing team, using CRM systems like Salesforce, only accesses client and marketing data.

To ensure enterprise information security, role segregation and the principle of least privilege control employee access levels. With increasing volumes of sensitive information, it is crucial not only to assign rights appropriately but also to monitor access to critical data. The next steps include classifying sensitive information, restricting access to critical resources, and implementing monitoring policies to oversee the actions of employees with elevated permissions.

For effective control, it is crucial to clearly identify sensitive data. Sensitive information includes data whose leakage could cause financial or reputational damage to the company, such as financial reports, personal data, corporate strategies, trade secrets, and technical documentation. Once identified, access to sensitive information should be restricted to employees who directly work with it. For instance, financial reports should be accessible only to the finance department, with access managed through systems like Microsoft Active Directory or Okta. Access policies define rules for handling sensitive information, including authentication, password changes, and user activity tracking. Monitoring tools like Splunk or SolarWinds help detect suspicious actions that may indicate unauthorized access attempts or data manipulation.

Access control methods for sensitive information provide reliable protection but require ongoing management to maintain effectiveness. Access restrictions

and activity monitoring form the foundation of security, but internal control is essential for comprehensive protection. It ensures transparency in access, anomaly detection, and adherence to security policies [3].

Internal control relies on policies and procedures that regulate data access, handling protocols, and security measures, including authorization requirements, rules for using sensitive data, and clear responsibility allocation. This minimizes the risk of violations and ensures all employees adhere to corporate standards. Regular monitoring detects abnormal activities that may signal threats or unauthorized access attempts. Automated systems analyze real-time activity, enabling quick responses to deviations. Logging and tracking user actions ensure transparency by recording all data access and modification activities, aiding both in incident investigation and in preventing recurrence.

Internal control and activity monitoring enhance transparency and enable rapid threat responses, but regular audits are essential for fully evaluating security policy effectiveness. Internal and external audits identify control weaknesses and provide an objective security assessment by independent experts. Internal audits are essential tools for assessing compliance with security policies and standards. Systems like Splunk and IBM QRadar facilitate regular checks to identify system weaknesses, evaluate logging and monitoring effectiveness, and ensure employees adhere to access rules for sensitive information. External audits, guided by standards such as ISO/IEC 27001 or conducted by auditing firms, provide an independent security assessment. External experts verify compliance with international standards and evaluate protective measures, offering new strategies to enhance security. It is recommended to conduct internal audits quarterly and external audits annually. Audit reports should include findings and recommendations for addressing any identified issues.

Regular internal and external audits provide objective security assessments and identify vulnerabilities. A strategic approach to access-related risk management forms a solid security foundation, enabling threat prediction and promoting a security culture. Risk management starts with identifying key threats and assessing their impact on information systems. Platforms like RSA Archer and ServiceNow classify risks by criticality, focusing on major threats such as unauthorized access, privilege abuse, and data leakage. This assessment guides a risk mitigation strategy with tools like Duo Security or Okta for multi-factor authentication, Microsoft Active Directory or CyberArk for access control, and Splunk or IBM QRadar for monitoring [4].

An essential aspect is staff training: employees should be familiar with security protocols and capable of protecting corporate resources. Programs like KnowBe4 and Proofpoint Security Awareness are used to raise security awareness. Regular reviews and policy updates with tools like AuditBoard or LogicManager help adapt protective measures to new challenges. Employee awareness is key–security training programs, seminars, and workshops reduce risks associated with human factors, fostering a culture of security within the organization.

Table 1.

Key Elements of a Comprehensive Access Security Approach

Element	*Description*	*Example Systems*
Account Management	Creation, deletion, and management of user access rights	Microsoft Active Directory, Okta
Password Policy	Setting password requirements, frequency of changes, and protection	LastPass, Keeper
Multi-Factor Authentication	Additional security through user identity verification	Duo Security, Google Authenticator
Role Segregation	Separation of key functions and access to prevent conflicts of interest	SailPoint, Cisco Identity Services Engine (ISE)
Access Control	Restricting access to resources based on user role and responsibilities	CyberArk, BeyondTrust
Risk Management	Risk assessment, classification, and mitigation related to access	RSA Archer, ServiceNow
Activity Monitoring	Tracking user actions to detect anomalies and potential threats	Splunk, IBM QRadar
Internal and External Audit	Checking compliance with security policies and standards, analyzing system vulnerabilities	AuditBoard, LogicManager
Employee Training	Increasing awareness and competencies in information security	KnowBe4, Proofpoint Security Awareness

Conclusions. Based on the analysis, it is recommended that companies regularly update access policies, implement multi-factor authentication, restrict access to critical data, and conduct information security training. Regular audits and monitoring help identify vulnerabilities in a timely manner. Modern approaches, such as using artificial intelligence for behavior analysis, adaptive authentication, and blockchain solutions for access management, enhance the protection of corporate resources. Companies that adopt the latest technologies will be able to effectively counter threats and maintain a high level of security.

Information sources

1. Panovyk U., Kutas S. (2024). Internet of Things for smart print production. Printing and Publishing, № 1(87). pp. 61–74. URL: https://doi.org/10.32403/0554-4866-2024-1-87-61-74

2. Mohamed A. K. Y. S. et al. (2022). A systematic literature review for authorization and access control: definitions, strategies and models. International Journal of Web Information Systems. URL: https://doi.org/10.1108/ijwis-04-2022-0077

3. Zubair M. et al. (2024). Access control for trusted data sharing. EURASIP Journal on Information Security. Vol. 2024, no. 1. URL: https://doi.org/10.1186/s13635-024-00178-z

4. Anton S. D. D. et al. (2021). The Global State of Security in Industrial Control Systems: An Empirical Analysis of Vulnerabilities around the World. IEEE Internet of Things Journal. 2021. pp. 1. URL: https://doi.org/10.1109/jiot.2021.3081741

УДК 004.056.55:004.932

ЗАХИСТ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

Кирило ЧЕПУРНОЙ
Лідія ТИМОШЕНКО
Національний університет "Одеська політехніка", м. Одеса, Україна.

Abstract. *The paper presents proposed recommendations and technical solutions to improve the existing protection system of a critical infrastructure facility. The recommendations are based on knowledge gained at the National University "Odesa Polytechnic" and practical skills acquired during work in the Odesa Regional State (Military) Administration.*

Key words: *critical infrastructure, martial law, cybersecurity, objects of protection.*

Анотація*. У роботі представлено запропоновані рекомендації та технічні рішення для удосконалення існуючої системи захисту об'єкту критичної інфраструктури. Рекомендації розроблені на основі набутих знань в Національному університеті "Одеська політехніка" та практичних навичок під час роботи в Одеській обласній державній (військовій) адміністрації.*

Ключові слова*: критична інфраструктура, воєнний стан, кібербезпека, об'єкти захисту.*

Теоретичні відомості

З 2014 року Україна перебуває у стані війни, фази якої змінюються. Найактивніше фаза бойових дій триває з 2022 року до сьогоднішнього дня. Незалежно від успіхів і поразок ворога на фронті – об'єкти критичної інфраструктури незалежно від їх географічного розташування постійно перебувають під загрозою. Такі об'єкти завжди є бажаною ціллю як фізичних так і для кібератак, що значно ускладнює їх захист.

Кібератаки є ключовою загрозою у будь-якому сучасному конфлікті. Вони призводять до дестабілізації функціонування критичної інфраструктури, що в свою чергу веде до руйнівних економічних, екологічних і соціальних наслідків. Сьогодні вимагає повного переосмислення розуміння всіх існуючих заходів кібербезпеки як військової, так і критичної цивільної інфраструктури. Консенсус про важливість кібератак у війнах 21-го століття існував вже давно, але справжні масштаби проблеми і її наслідки на жаль виявились недооціненими.

Одеська обласна державна (військова) адміністрація (ОВА) – ключова державна інституція виконавчої влади і ланка в системі державного управ-

ління, особливо в умовах воєнного стану. ОВА виступає координатором роботи органів влади, органів місцевого самоврядування, критичних підприємств державного і приватного сектора в регіоні. Також на обласну адміністрацію покладено задачі з оборонної роботи. У контексті воєнного стану роль у мирний час державної, а тепер – військової адміністрації посилилась, адже до її основних функцій відносять реагування на надзвичайні ситуації, розробку і реалізацію заходів безпеки.

Актуальність кібербезпеки критичної інфраструктури під час війни обумовлена не лише постійною зовнішньою загрозою, а й необхідністю періодичного навчання персоналу і розробки нових сучасних стратегій захисту.

Запропоновані заходи програмно-апаратного характеру і технічні засоби захисту

У реаліях сьогодення, враховуючи щоденно зростаючу кількість кіберзагроз, об'єкти критичної інфраструктури, зокрема й Одеська обласна військова адміністрація, потребують надійних та безпечних сертифікованих рішень для забезпечення захисту своєї інформаційної інфраструктури. Використання обладнання на архітектурі Cisco є одним із найкращих варіантів, оскільки йому притаманні: широкий асортимент рішень; сумісність та інтеграція; інновації; навчання та технічна документація; високий рівень безпеки; легкість масштабування; стабільність і надійність; Одним з найважливіших факторів на користь вибору обладнання Cisco є те, що це американська компанія, яка за сприяння американського уряду активно підтримує гуманітарні ініціативи, направлені на надання допомоги Україні в умовах військового конфлікту. До такої підтримки відносять таке: безоплатна технічна підтримка; безоплатне надання техніки і технічних рішень; навчальні програми для фахівців; активне партнерство з державними структурами.

Обладнання Cisco є одним з найбільш поширених рішень на світовому ринку, що відкриває можливості для отримання обладнання цієї компанії не тільки шляхом прямих постачань від виробника і американського уряду, а й від великої кількості благодійників і урядів країн-союзниць. Надлишок необхідного обладнання дозволяє зібрати необхідні апаратні рішення з мінімальними затратами, а партнерство з компанією Cisco максимально вирішує як фінансові, так і часові затрати на навчання персоналу.

Для підвищення рівня захищеності об'єкту критичної інфраструктури необхідно:

а) серверне обладнання;

б) мережеве рішення;

в) комплексне рішення мережевої безпеки;

г) система керування та моніторингу;

г) система віртуалізації та інтеграції обчислювальних ресурсів.

Для закриття цих потреб потрібне надійне обладнання з можливістю масштабування системи, легкою інтеграцією в існуючу систему і сертифікацією безпеки найвищого рівня. Отже, пропонується наступне:

а) серверне обладнання: Cisco UCS C240 M6 Rack Server, Cisco Catalyst 9300 Series Switches;

б) мережеве рішення: Cisco Meraki MX250;

в) комплексне рішення мережевої безпеки: Cisco Firepower 2130 NGFW, Cisco Identity Services Engine;

г) керування і моніторинг: Cisco DNA Center Appliance DN2-HW-APL;

ґ) система віртуалізації та інтеграції обчислювальних ресурсів: Cisco HyperFlex HX240c M5.

Вартість зазначеного обладнання в максимальній комплектації за 1 шт. знаходиться в діапазоні від 6 до 80 тис. $ за нову одиницю і відповідає наступним стандартам і має сертифікати безпеки: Common Criteria (CC), FIPS 140-2, SOC 2 Type II, ISO/IEC 27001.

Враховуючи особливості воєнного часу, захист об'єкту критичної інфраструктури не повинен обмежуватись територією самого об'єкту. Варто завжди допускати можливість фізичної атаки на об'єкт, або спроби незаконного проникнення на його територію. Враховуючи це, для побудови широкої мережі зовнішнього і внутрішнього відеоспостереження пропонується наступне:

а) зовнішнє відеоспостереження: Cisco Meraki MV72, Cisco Video Surveillance 8030;

б) внутрішнє відеоспостереження: Cisco Meraki MV22;

в) ПЗ для централізованого управління системою відеоспостереження: Cisco Meraki Dashboard.

Вартість зазначеного обладнання в максимальній комплектації за 1 шт. становить в діапазоні від 1300 до 2500 $ за нову одиницю і відповідає наступним стандартам і має сертифікати безпеки: ISO/IEC 27001, FIPS 140-2, SOC 2 Type II, CSA STAR.

Висновки. На основі аналізу воєнно-політичної, економічної ситуації в країні, актуальних загроз, особливостей функціонування об'єкту критичної інфраструктури в умовах воєнного стану, врахувавши високий рівень взаємодії з міжнародними партнерами, фондами, союзними державами, вивчення ринку обладнання на відповідність параметрам і викликам, запропоновано технічні рішення, впровадження яких здатне підвищити рівень захисту будь-якого об'єкту критичної інфраструктури. У роботі наведено обґрунтування доцільності використання наведеного обладнання, реальні перспективи і можливі шляхи його отримання, чи придбання.

УДК 004.056+621.396

СТРАТЕГІЇ РЕАЛІЗАЦІЇ ЗАХОДІВ КІБЕРБЕЗПЕКИ В АРХІТЕКТУРІ IIoT ПОЛІГРАФІЧНОГО ПІДПРИЄМСТВА

Ігор ТАНЧИН
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *On the basis of the determined levels of the layered architecture of the industrial Internet of Things, the consequences of cyberattacks and identified countermeasures for the implementation of a comprehensive cyber security strategy of a modern printing company are investigated.*
Keywords*: cyber security of industrial infrastructure, IIoT architecture, Industry 4.0, telemetry, printing company.*

Анотація. *На основі обумовлених рівнів пошарової архітектури промислового інтернету речей досліджено наслідки кібератак та виокремлені контрзаходи для реалізації комплексної стратегії кібербезпеки сучасного поліграфічного підприємства.*
Ключові слова*: кібербезпека промислової інфраструктури, архітектура IIoT, Індустрія 4.0, телеметрія, поліграфічне підприємство.*

Впровадження промислового інтернету речей (IIoT) створює значні можливості для оптимізації поліграфічного виробництва, але разом з тим підвищує рівень загроз фізичної безпеки. Реалізація заходів безпеки потребує комплексного підходу, який включає технологічні рішення, такі як шифрування і IDS, організаційні заходи, як-от сегментація мереж і політика доступу, а також розвиток корпоративної культури безпеки через навчання і підвищення обізнаності співробітників. Надійний кіберзахист дозволяє поліграфічним підприємствам мінімізувати втрати і підвищити рентабельність.

Наслідки кібератак на технології IIoT найкраще досліджувати на пошарованій моделі [1], яка складається з трьох основних рівнів: рівня сприйняття, мережевого рівня та прикладного рівня. Кожен із цих рівнів має свій набір вразливостей і типових атак, хоча деякі з атак можуть охоплювати кілька рівнів одночасно. На рисунку показані обумовлені рівні та основні види атак, характерні для кожного з них.

Інтерфейсом між фізичним світом та IIoT-пристроями поліграфічного підприємства є рівень сприйняття. На цьому рівні відбуваються всі процеси збору телеметрії через сенсори, а також дії, які пристрої виконують на основі взаємодії з довкіллям. Зібрані дані передаються на мережевий рівень, а команди для виконання приймаються з нього. Категорія фізичних атак на цьому рівні охоплює всі деструктивні дії, спрямовані на апаратне забезпечення IIoT-пристроїв. Зазвичай передбачається, що зловмисник має фізичний доступ до пристрою, може замінити або пошкодити його компоненти

для отримання доступу до конфіденційної інформації (*наприклад*, паролів користувача) або для відключення певних функцій. Прикладами іншої категорії атак з підробкою особистості є спуфінг (коли зловмисник використовує чужу ідентичність) або атаки Сібіл (створення великої кількості фальшивих ідентичностей). Такі атаки часто проходять успішно при відсутності механізмів автентифікації, особливо на етапі налаштування IIoT-пристроїв, *наприклад*, коли зловмисник видає себе за підроблену точку доступу Wi-Fi.

Метою мережевого рівня є забезпечення зв'язку між IIoT-пристроями, а також їх підключення до Інтернету. На цьому рівні передаються зібрані дані від рівня сприйняття до рівня додатків і навпаки. Основні технології включають бездротові протоколи зв'язку і шлюзи, які з'єднують локальні IIoT-мережі з більшими мережами, такими як Інтернет. Відповідно, атаки на цьому рівні можуть бути спрямовані як на мережеві компоненти, так і на проміжні елементи системи. Категорія атак типу MitM перехоплює конфіденційну інформацію шляхом втручання у зв'язок між двома законними учасниками. Іноді зловмисник також змінює дані перед тим, як переслати їх далі. До таких категорії атак часто входять атаки повтору (replay), коли перехоплені повідомлення повторно відправляються або затримуються для досягнення певних цілей. У випадку атак на маршрутизацію зловмисник намагається порушити доступність локальної мережі, розповсюджуючи хибну інформацію про маршрути або перериваючи потік даних (рис. 1).

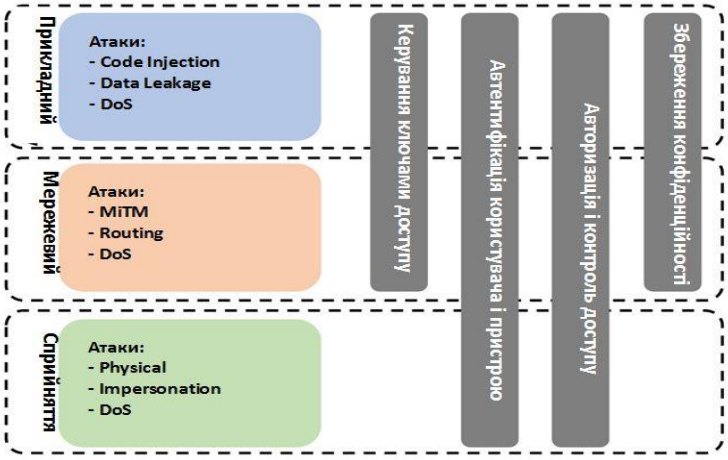


Рисунок 1 – Рівні IIoT з категоріями атак та їх контрзаходами [1]

Прикладами є атаки категорії "сінкхол" (sinkhole), де зловмисник "поглинає" повідомлення у багатоступеневій мережі, і вибіркове пересилання, коли зловмисник відфільтровує певні повідомлення, пропускаючи лише деякі з них.

Прикладний рівень відповідає за надання різних сервісів з яких складаються IoT-застосунки. Він працює на основі даних, зібраних на рівні сприйняття, і забезпечує взаємодію через мережевий рівень. На відміну від попередніх обумовлених рівнів, прикладний рівень може розвиватися завдяки оновленням програмного забезпечення, часто без значних змін у підсистемах. Захист цього рівня є досить складним завданням, оскільки нові вразливості можуть виникати з кожним оновленням програмного забезпечення. Категорія атак ін'єкції шкідливого коду передбачає, що зловмисник успішно вводить деструктивний скрипт. Використовуючи вразливість, він отримує контроль над зараженим пристроєм. Можливі цілі таких атак включають використання пристроїв для розподіленої атаки типу відмова в обслуговуванні (DDoS), коли велика кількість IoT-пристроїв перевантажує сервер запитами; несанкціоноване використання обчислювальних ресурсів пристрою (криптоджекінг) для майнінгу криптовалюти; вимагання через програмне забезпечення-здирник, яке шифрує дані користувача з метою вимагання викупу. Категорія витоку даних використовує вразливості у програмному забезпеченні та налаштуваннях сервісів для крадіжки конфіденційної інформації. *Наприклад*, атака на неправильно налаштовані хмарні сервіси може призвести до несанкціонованого доступу до персональних даних.

Окремою гіперкатегорією є мультирівневі атаки. Так, деякі мультирівневі атаки можуть виникати на кількох рівнях еталонної моделі IoT, спричиняючи різні наслідки. У цій категорії основним прикладом є атаки типу відмова в обслуговуванні (Denial-of-Service, DoS). З точки зору користувача атака DoS означає недоступність певного ресурсу або сервісу, що зазвичай досягається шляхом перевантаження пристроїв надмірною кількістю запитів.

З архітектурної точки зору, проте, важливо розрізняти, на якому рівні еталонної моделі IIoT виникає атака DoS, щоб вжити відповідних контрзаходів. На рівні сприйняття мультирівневі атаки DoS здебільшого виражаються у вигляді заглушення сигналу, що порушує бездротовий зв'язок або можливості виявлення IIoT-пристроїв. Такі атаки також можуть спрямовуватись на доступність окремого обладнання, *наприклад*, шляхом перевантаження їхніх обмежених за ресурсами процесорів. На мережевому рівні атаки DoS націлені на комунікаційну інфраструктуру, що може призвести до тимчасового відключення пристроїв, *наприклад*, шляхом навмисного перевантаження маршрутизаторів. На прикладному рівні атаки DoS зосереджуються на критичних сервісах, *наприклад*, шляхом надсилання великої кількості запитів, що ставить під загрозу доступність важливих (індустріальних) процесів, які залежать від цього сервісу.

Для реалізації стратегії кібербезпеки поліграфічного підприємства вирішено застосовувати низку рішень, які включають різні технічні та організаційні заходи. Одним із основних криптографічних методів захисту даних

при автентифікації є шифрування. Завдяки використанню симетричних та асиметричних схем шифрування можна забезпечити конфіденційність даних. У контексті промисловості використання легких протоколів автентифікації дозволяє зменшити навантаження на пристрої і підтримувати безпеку з мінімальними затримками.

Оновлення програмного забезпечення є важливою складовою захисту від загроз. Система автоматизованих оновлень та управління патчами може зменшити ризик використання вразливостей у довготривалих компонентах IIoT. Необхідно також залучити механізми, які дозволяють виявляти вразливості і тестувати оновлення в неробочий час для збереження працездатності системи.

Сегментація мережі дозволяє обмежити доступ до критичних ресурсів. *Наприклад*, політика обмеженого доступу для конкретних пристроїв знижує ризик несанкціонованого проникнення в мережу. Використання методів безпечного виконання, таких як ARM TrustZone, дозволяє надійно ізолювати критичні функції пристроїв, застосовуючи контроль доступу.

Моніторинг трафіку мережі та системи виявлення вторгнень і інших аномалій дозволяють своєчасно виявляти підозрілу активність, запобігаючи поширенню загроз. Оскільки мережевий трафік у промислових середовищах має характерні регулярні шаблони і патерни, аномалії в трафіку можна алгоритмічно виявляти, що дозволяє швидко реагувати на загрози.

Напевно найважливішим аспектом безпеки IIoT є людський фактор. Регулярні тренінги з кібербезпеки допомагають персоналу краще розуміти ризики та правильно реагувати на інциденти. Підвищення обізнаності співробітників поліграфічного підприємства також сприяє зниженню ризику внутрішніх загроз.

Висновки. Таким чином, реалізації заходів кібербезпеки в архітектурі IIoT поліграфічного підприємства потребує комплексного підходу, який включає технологічні рішення на кожному обумовленому рівні. Подальший розвиток проєкту буде зосереджений на масштабуванні корпоративного сервера відповідно до концепції Індустрії 4.0-5.0, придатного для комплексного розгортання промислових платформ Інтернету речей, зокрема при прогнозованому технічному обслуговуванні машинного парку оперативної поліграфії [2].

Інформаційні джерела

1. Gargula N. Applications of an industrial internet of things based on the perspective of cyber-physical systems. International Journal of Creative Research Thoughts, Vol.10 (5), 2022. – С. 20–27.

2. Танчин І. Методи технічного обслуговування промислового поліграфічного обладнання. Тези доповідей студентської наукової конференції Української академії друкарства. Львів, 2024.

УДК 004.056

ТЕХНОЛОГІЯ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ ДОВІРИ ТА ПРОЗОРОСТІ У ДЕРЖАВНИХ РЕЄСТРАХ

***Валерія БАЛАЦЬКА*[1]**
***Іван ОПІРСЬКИЙ*[2]**

[1]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.
[2]Кафедра захисту інформації Національного Університету "Львівська Політехніка", м. Львів.

Abstract. *Implementing blockchain technologies in state registers contributes to increasing the transparency and security of information, reducing corruption risks, and increasing citizens' trust in state structures. This work examines the prospects of blockchain technologies in public administration to ensure data immutability and information confidentiality.*

Keywords: *personal data protection, blockchain, government registries, transparency, data security, privacy, smart contracts, audit, personal data.*

Анотація. *Впровадження блокчейн-технологій у державні реєстри сприяє підвищенню прозорості та безпеки інформації, а також зниженню корупційних ризиків і підвищенню довіри громадян до державних структур. Дана робота розглядає перспективи блокчейн-технологій у державному управлінні для забезпечення незмінності даних і конфіденційності інформації.*

Ключові слова: *захист персональних даних, блокчейн, державні реєстри, прозорість, безпека даних, конфіденційність, розумні контракти, аудит, персональні дані.*

Сучасні інформаційні технології, зокрема блокчейн, здатні суттєво трансформувати державні реєстри, підвищивши їх ефективність, прозорість та надійність. Державні реєстри є основою для надання адміністративних послуг, зокрема реєстрації права власності, шлюбу, розірвання шлюбу, актів цивільного стану, інформації про підприємства тощо [1, 2]. Проте традиційна централізована структура управління реєстрами створює кілька значних ризиків, як-от вразливість до кібератак, корупція, ризики несанкціонованого доступу до даних і обмеження прозорості операцій, що підриває довіру до державних органів.

Одним із способів подолання цих проблем є впровадження блокчейн-технологій, завдяки яким можлива децентралізація, незмінність і підвищення прозорості записів. Блокчейн-технології зберігають інформацію у формі незмінних записів, що захищені криптографічними методами та підтверджуються мережею незалежних учасників. Така структура забезпечує високу надійність даних, оскільки записи неможливо змінити або видалити без згоди всіх учасників мережі. Це підвищує прозорість роботи державних реєстрів і дозволяє відстежувати всі зміни даних, що запобігає корупційним маніпуляціям.

Блокчейн-технологія забезпечує підвищений захист персональних даних завдяки розподіленому зберіганню інформації та децентралізованому доступу. Така модель ускладнює можливість несанкціонованого доступу до конфіденційної інформації, оскільки відсутній єдиний центральний сервер, який можна атакувати. Крім того, використання смарт-контрактів в блокчейн дозволяє автоматизувати процеси доступу до даних і управління правами доступу, що додатково підвищує рівень безпеки [3].

Відповідно до міжнародних стандартів захисту даних, таких як Загальний регламент про захист даних (GDPR), блокчейн може бути адаптований для дотримання прав користувачів на конфіденційність і контроль над власними даними. Смарт-контракти дозволяють автоматично забезпечувати відповідність нормативним вимогам шляхом контролю за доступом до даних та забезпечення конфіденційності інформації. Крім того, блокчейн надає можливість зберігати персональні дані у розподіленому середовищі, що суттєво ускладнює несанкціонований доступ і підвищує безпеку збереженої інформації [5].

Прозорість є однією з ключових переваг блокчейн-технологій. Усі зміни у записах блокчейн можна відстежити завдяки їх зберіганню у вигляді послідовності блоків, де кожен блок містить хеш попереднього блоку. Це унеможливлює зміни без згоди всієї мережі. Завдяки цьому у державних реєстрах забезпечується прозорість даних, що дає можливість громадянам і державним органам проводити аудит кожної операції [4]. Це не тільки знижує корупційні ризики, але й підвищує довіру до роботи державних структур.

Наприклад, у реєстрах нерухомості записи можна зробити прозорими та доступними для перевірки громадянами. Це дозволяє забезпечити повну відкритість даних і уникнути маніпуляцій з правами власності. Таким чином, застосування блокчейн-технології може бути ефективним інструментом для боротьби з корупцією, оскільки забезпечує відкритий доступ до даних для всіх зацікавлених сторін.

Попри значний потенціал блокчейн в державному секторі, його впровадження супроводжується рядом технічних і фінансових викликів. Зокрема, високі витрати на впровадження блокчейн-систем, необхідність навчання персоналу та адаптації існуючих реєстраційних систем є важливими бар'єрами для реалізації. Питання масштабованості блокчейн також залишається актуальним, оскільки великі реєстраційні системи потребують високої швидкості обробки даних, яку важко забезпечити через процес підтвердження транзакцій у блокчейн [5].

Проте довгострокові вигоди можуть значно перевищувати початкові витрати. Зокрема, блокчейн може підвищити прозорість державних реєстрів, знизити витрати на аудит і покращити рівень довіри громадян до державних структур. Для підвищення ефективності цієї технології важливим напрямом є створення пілотних проєктів та тестування різних моделей реалізації з урахуванням специфіки кожного державного реєстру.

Висновки. Блокчейн-технологія має великий потенціал для трансформації державних реєстраційних систем, забезпечуючи їхню прозорість, надій-

ність і захист персональних даних. Використання блокчейн може значно підвищити ефективність і довіру громадян до державних органів, забезпечуючи незмінність і захищеність даних, доступність інформації для аудиту та прозорість операцій. Впровадження цієї технології потребує ретельного планування і врахування як технічних, так і правових аспектів, однак може стати важливим кроком у розвитку сучасної цифрової держави.

Інформаційні джерела

1. Балацька В. С., Опірський І. Р., Побережник В. О. Використання Non-Fungible Tokens та блокчейн для розмежування доступу до державних реєстрів // Кібербезпека: освіта, наука, техніка. – 2024. – № 4 (24). – С. 99–114. URL: https://doi.org/10.28925/2663-4023.2024.24.99114.

2. Опірський І., Балацька В., Побережник В. Сучасні можливості використання блокчейн-технології в освітній системі // Ukrainian Scientific Journal of Information Security. – 2023. – Vol. 29, Issue 3. – С. 138–146. URL: https://doi.org/10.18372/2225-5036.29.18073.

3. Побережник В., Балацька В., Опірський І. Розробка концепції системи управління навчанням на основі блокчейн-технології // CEUR Workshop Proceedings. – 2023. – Vol. 3550.

4. Balatska Valeriia, Opirskyy Ivan, Slobodian Nataliia, Blockchain for enhancing transparency and trust in government registries, CPITS-II 2024: Cybersecurity Providing in Information and Telecommunication Systems II. – 2024. pp. 50–59.

6. Poberezhnyk V., Balatska V., Opirskyy I. Development of the Learning Management System Concept based on Blockchain Technology, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023). pp. 143–156.

УДК 621.372

ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ КОГНІТИВНОЮ СИСТЕМОЮ ОСОБИ В УМОВАХ ДІЇ АКТИВНИХ ЗАГРОЗ

***Наталія ЛИСА*[1]**
***Ростисла ТКАЧУК*[2,1]**
***Олег СИДОРЕНКО*[1]**

[1]Національний університет "Львівська політехніка", м. Львів, Україна.
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.

Abstract. *Analysis of the mechanisms of activity of individuals and teams of performers in extreme situations, as well as forecasting possible failures in the decision-making process due to mental tension, is an urgent problem. The processes of solving tasks and problems form the basis of both the subconscious and conscious components of intellectual activity, so it is important to develop the concept of identifying the mechanisms of mental (intellectual) activity of the individual.*

Key words*: information, identification, processes of intellectual activity, effects of threats on the cognitive system.*

Анотація. *Аналіз механізмів діяльності в ІАСУ особистості та команд виконавців в екстремальних ситуаціях, а також прогнозування можливих збоїв у процесі прийняття рішень через психічну напруженість, є актуальною проблемою. Процеси розв'язання завдань і проблем становлять основу як підсвідомої, так і свідомої складової інтелектуальної діяльності, тому важливим є розробка концепції ідентифікації механізмів розумової (інтелектуальної) діяльності особистості.*

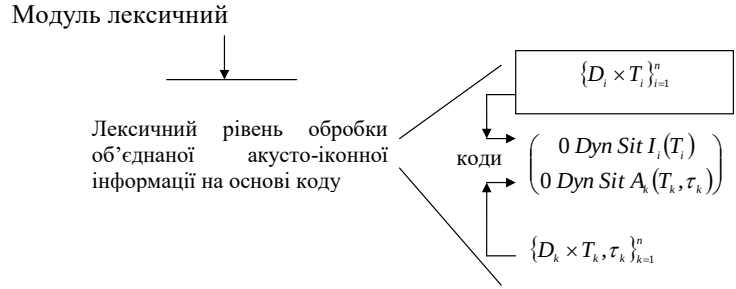
Ключові слова: *інформація, ідентифікація, процеси інтелектуальної діяльності, дії загроз на когнітивну систему.*

Концепція Конемана розумового зусилля, як уваги в процесі розв'язання ієрархії проблемних задач, яка ґрунтується на оцінці інтелектуального ресурсу необхідного для розв'язання проблемної ситуації в кожен момент часу. Активізація розумового (інтелектуального) зусилля визначається складністю задачі в ієрархії проблем, які необхідно розв'язати. При зростанні рівня складності задачі відбувається ріст активізації до певної межі, після якої вже не відбувається росту інтелектуальних ресурсів і починаються логіко-функціональні збої в процедурах прийняття рішень, що приводить до помилок в процесі виконання управління діями. Тобто увага виступає як спосіб регулювання та оволодіння особою власної поведінки усвідомлено, як на основі натурального підсвідомого розвитку так і науково-культурного, з врахуванням набутих знань.

Гальперін П. розглядав увагу, як внутрішній контроль за поведінкою і вважав, що вона є ідеальною, звернутою і автоматизованою цілеорієнтованою дією, тобто розвитком процесів контролю від свідомих до автоматизованих дій. При цьому структура процедур прийняття рішень є скритою для зовнішнього спостереження. Звідси випливає, що увага є феноменальне продуктивне проявлення роботи ведучого рівня інтелектуальної структури в організації діяльності особи, орієнтованої на досягнення мети.

Визначимо основні функціональні модулі в цілеорієнтованій структурі нейропроцесора, які виконують відповідно до типу даних і цілей A_i – операції, перетворення, трансакції:

$$N_i = \{1\ldots12\};\ A_i \to \{D_i \times T_i\}_{i=1}^{n}\ \ T_i = \{0;0,3;0,7;1,0\}\,\text{с}$$



Модуль концептуальний – функціонує на основі семантичного коду.

Робота лексичного модуля забезпечується системою логогенів, структур спеціалізованих для опрацювання слів. В ньому проходить інтеграція фонологічних і орфографічних характеристик образу ситуації для створення моделі об'єкта.

Іконічний блок пов'язаний з функціонуванням образного сенсорного перетворювача на основі образного коду:

$$\left(I\left(\vec{x},t\right)\right) \rightarrow Odyn\ Sit\ I_k\left(T_i\right)$$

та його відображенні в образній оперативній пам'яті у вигляді букв, слів, патернів, ікон.

Розглянемо структурну схему процесу обробки даних при формуванні образів ситуацій (рис. 1) [1].

Існують дві системи обробки інформації згідно концепції Величковського Б. та репрезентації знань Коселин:

– виділення глобального просторового каркасу видимої сцени у вигляді зорового модального буфера;

– операції специфікуючі внутрішню структуру сцени і окремих об'єктів в ній, на основі використання амодальної асоціативної пам'яті, в якій зберігаються описи класів об'єктів та їх назв, що є основою класифікації потоку інформаційних образів.

Відбір інформації проходить з допомогою сенсорів (рецепторів), які перетворюють вхідні енергетичні збурення різної фізичної природи в електричний сигнал [2].

Опрацювання інформації відбувається з використанням:

– ефекторів, які обробляють інформацію від сукупності ефекторів та коректують їх характеристики залежно від рівня збудження;

– пам'яті, як структури для зберігання імунно-природної інформації та динамічних даних від рецепторів (сенсорів).

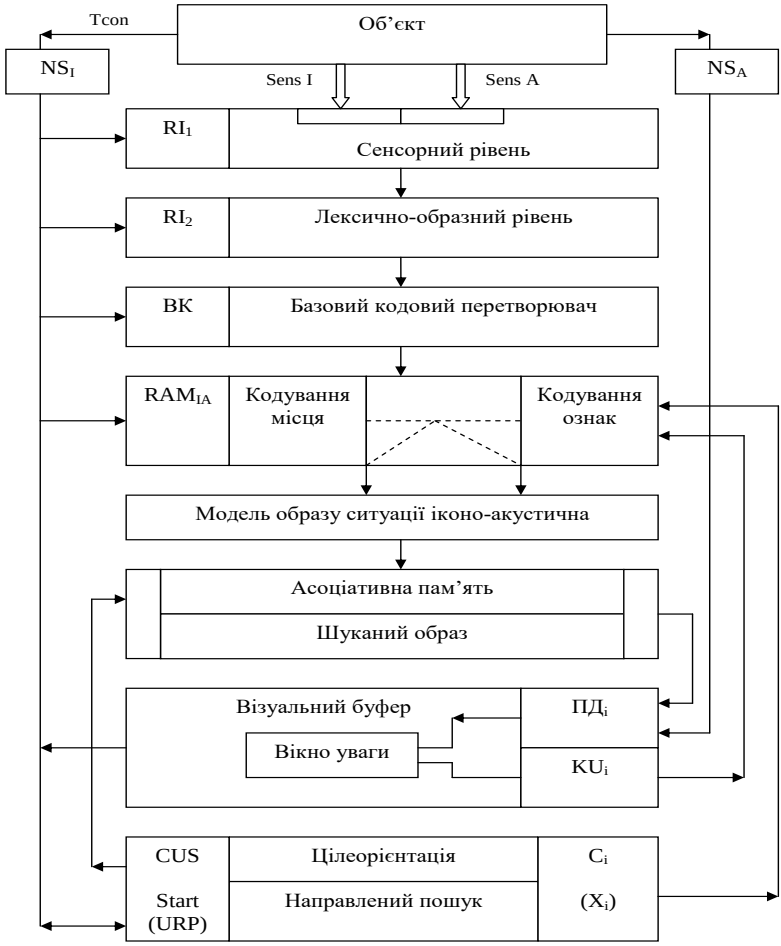


Рисунок 1 – Структурна схема формування образів ситуацій, де: C_i – цільова координата, (x_i) – потік даних про траєкторію руху, *CUS* – цілеспрямована система, *Strat(URP)* – стратегія управління розв'язання проблеми, KU_i – команди управління, $ПД_i$ – потік даних про ситуацію.

В пам'яті зберігаються дані:
– структуровані відносно реакції на збурення;
– інформація про зовнішні і внутрішні енергоресурси;
– програми опрацювання вхідних даних;
– про результати реакції на збурення;
– інформація від сенсорів.

Концептуальний рівень – обробки інформації ґрунтується на основі використання структурованих знань в процедурах прийняття рішень.

Прийняття рішень згідно цілеорієнтації вимагає, на основі одержаних даних про стан об'єкта та динамічну ситуацію, їх опрацювання, тобто виконання над ними логічних й обчислювальних операцій відповідним процесором за програмою згідно алгоритму і стратегії досягнення мети. Тобто прийняття рішень ґрунтується на системі знань, її структурній стабільності і динамічності поповнення та використання [3].

Структурна стабільність і динамічність знань виражає їх репрезентативність, тобто:

– репрезентації типи з пропозиціональною структурою;

– репрезентації часові динамічні, як форми представлення ситуацій;

– знання з відповідно означеною логіко-математичною структурою (конструктивні);

– модулі фіксованої і просторової пам'яті.

Знання переробляються та використовуються (актуалізуються) у відповідності з цілями, що стоять перед цілеспрямованою особою.

Семантичний код лежить в основі пам'яті і є організуючим для структури знань, а також є носієм інформації про динамічну настройку сенсорно-модальної і короткочасної пам'яті. На основі семантичних ознак і єдиного формату блоків знань, які формуються концепти різних об'єктів.

Функціонування концептуальних знань визначається цільовою орієнтацією згідно поставленої мети розв'язання проблемної задачі:

– розуміння сенсу тексту;

– формування програми дій;

– синтезу алгоритму виконання управлінських дій здатних привести до досягнення мети.

Концептуальні репрезентації – констатують знання про навколишній світ і виражаються через предикативні логічні структури мови (декларації).

Образні репрезентації – відображають просторові характеристики форми об'єктів, розмір і орієнтацію відносно базису (декларативні знання).

Репрезентації дії – знання про методи і способи цілеорієнтованих дій, їх значення, спосіб виконання (процедурне представлення).

Вище наведене лежить в основі розподілу пам'яті на процедурну і декларативну. Когнітивна переробка потоків інформації включає як декларативну так і процедурну компоненти. Для активізації декларативного знання необхідне усвідомлення проблеми, а процедурні знання виконуються на автоматизмі дій. При цьому декларативні знання можуть переходити в процедурні по мірі настання навиків автоматизації. Для цих двох форм знань є необхідною суб'єктивна орієнтація на проблемно-цільову задачу.

Виходячи з концепції Гульвінга, можна виділити такі види пам'яті:

– оперативна короткотривала;

– довготривала без структуризації даних;

– концептуальна впорядкована довготривала;

– автобіографічна ментальна репрезантивна;

– метапам'ять і ефективні стратегії індивідуального запам'ятовування даних і образів ситуацій.

А це, відповідно, і є елементом синтезу нейропрцесорів.

Висновки. З використанням елементів теорії інтелекту та когнітивної психології вивчаються моделі прийняття рішень у людино-машинних інтегрованих системах. Це дає можливість обґрунтувати процедури тестування осіб та оцінки їх здатності приймати управлінські рішення як в умовах нормальних, так і в екстремальних ситуаціях.

Інформаційні джерела

1. Дурняк Б. В., Сікора Л. С., Антоник М. С., Ткачук Р. Л. Когнітивні моделі формування стратегій оперативного управління інтегрованими ієрархічними структурами в умовах ризиків і конфліктів. Львів: Українська академія друкарства, 2013. 449 с.

2. Сікора Л. С. Когнітивні моделі та логіка оперативного управління в ієрархічних інтегрованих системах в умовах ризику. Львів: ЦСД, 2009. 432 с.

3. Ткачук Р. Л., Сікора Л. С. Логіко-когнітивні моделі формування управлінських рішень інтегрованими системами в екстремальних умовах: посібник. Львів: Ліга–Прес, 2010. 404 с.

УДК 621.372

ІНТЕЛЕКТУАЛЬНІ ТА ПСИХОЛОГІЧНІ ХАРАКТЕРИСТИКИ ОСОБИ ЯК УПРАВЛІНСЬКОГО ЕЛЕМЕНТУ ІНТЕГРОВАНИХ СИСТЕМ

***Любомир СІКОРА*[1]**
***Наталія ЛИСА*[1]**
***Ростислав ТКАЧУК*[2, 1]**
***Ольга ФЕДЕВИЧ*[1]**

[1]Національний університет "Львівська політехніка", м. Львів, Україна.
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.

Abstract*. The integrated management system (ICS) is represented by a joint functional goal-oriented activity of hierarchically related structures, both machine and information systems, as well as teams of operators and managers. They carry out management activities for the implementation of the target tasks of the organization, enterprise, complex energy structure and economic structure within the region, the state.*

Keywords: *person, intellect, structure, management, integration, information systems.*

Анотація. *Інтегрована управлінська система (ІУС) представлена спільною функціональною цілеорієнтованою діяльністю ієрархічно пов'язаних структур, як машинних та інформаційних систем так і команд операторів і керівників. Вони виконують управлінську діяльність заради реалізації цільових завдань організації, підприємства, складної енергоструктури та господарської структури в рамках регіону, держави.*

Ключові слова: *особа, інтелект, структура, управління, інтеграція, інформаційні системи.*

Проблема кібербезпеки техногенної інфраструктури є компонентою соціальної і державної інтегрованої системи з складною ієрархією управління. Визначальна роль в таких системах припадає на інтелектуальний потенціал верхнього рівня ієрархії, тобто на управлінську команду з високим рівнем професіональної, наукової підготовки та цілеорієнтованої на забезпечення ефективних рішень в рамках всієї інфраструктури. Відповідно ставляться високі вимоги до рівня підготовки персоналу та методів відбору креативних кадрів здатних приймати рішення в кризових умовах. В основу процедури відмови мають бути закладені сучасні концепції побудовані на логіко-когнітивних моделях діяльності особи.

*1. Управління техногенною інфраструктурою в умовах загроз***.** На ефективність функціонування складних систем впливає [1]: забезпечення ресурсами (матеріальними, енергетичними, інформаційними, фінансовими); інтелектуальний рівень персоналу; база знань з технології виробництва і управління; стратегія і тактика прийняття рішень на управління ІУС для досягнення мети в умовах дії загроз і конфліктів спровокованих на ринках; психологічні умови забезпечення цілісного функціонування апарату управління і виконавського колективу.

У психології управління базовою концепцією [1–6] є людський фактор, як сукупність психофізичних та інтелектуальних характеристик особи здатної приймати і виконувати рішення. Тому актуальною є проблема побудови моделі особи, вивчення психічних та інтелектуальних функцій людини, формування нею стратегій прийняття цільових рішень та тактик дій. Ці моделі повинні ґрунтуватись на таких принципах [1, 5–7]:

– принцип еволюційного розвиту;

– принцип об'єктивності (точність, обґрунтованість, надійність, достовірність) в процесі формування висновків;

– наукова аргументованість висновків на основі проведених досліджень та адекватність методів дослідження проблеми і об'єкту;

– принцип системності, як виділення системоутворюючої властивості, яка об'єднує елементи системи в одне ціле через зв'язки в структурі, що здатна реалізувати досягнення мети при наявних інформаційних та енергетичних ресурсах;

– принцип комплексності дослідження з використання всебічних знань про елементи і характеристик об'єкта дослідження.

В ІУС найбільш складним елементом є особа і тому побудова моделей її діяльності є актуальною.

2. Особа як цілеорієнтована інтелектуальна система (CIS) та її інтелектуальні ознаки. Мотивація – це різні за протяжністю та силі прояви, які актуалізуються під впливом особливих ознак ситуації, зовнішніх умов і змушують людину діяти в певному напрямку [6–7]. Мотив – це спонукання до діяльності під впливом цілеорієнтуючих факторів. Виступає як індивідуальна ознака особи при дії в стандартних умовах. Схему діяльності можна виразити у вигляді структури зображеної на рисунку 1.

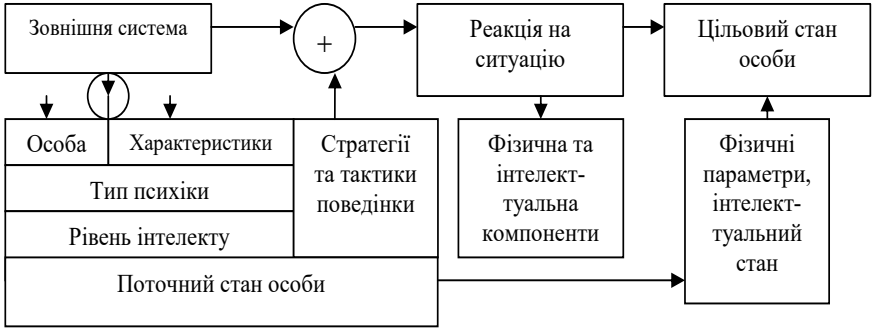


Рисунок 1 – Структурна схема дії особи в стандартних умовах

Відповідно види цілеорієнтованих мотивів особи поділяються на:
– прагнення до успіху і подолання перепон;
– обминання невдач, самолюбство;
– прагнення до дружніх відносин в колективі;
– агресія в колективнім середовищі; автономія відносно колективу;
– підкорення авторитету, лідеру;
– домінування, прагнення влади в суспільстві;
– обминання небезпек;
– мазохізм, самобичування, самоприниження;
– виправдання неправильних дій.

Етапи дій включають ланцюг від постановки проблеми до пошуку операціональних способів виконання цільових дій. Дія – одна із компонент діяльності особи, яка формується під впливом необхідності досягнення усвідомленого результату, цілі та включає такі компоненти: орієнтацію, виконання, контроль. В структуру дії входять елементи, зображені на рисунку 2.

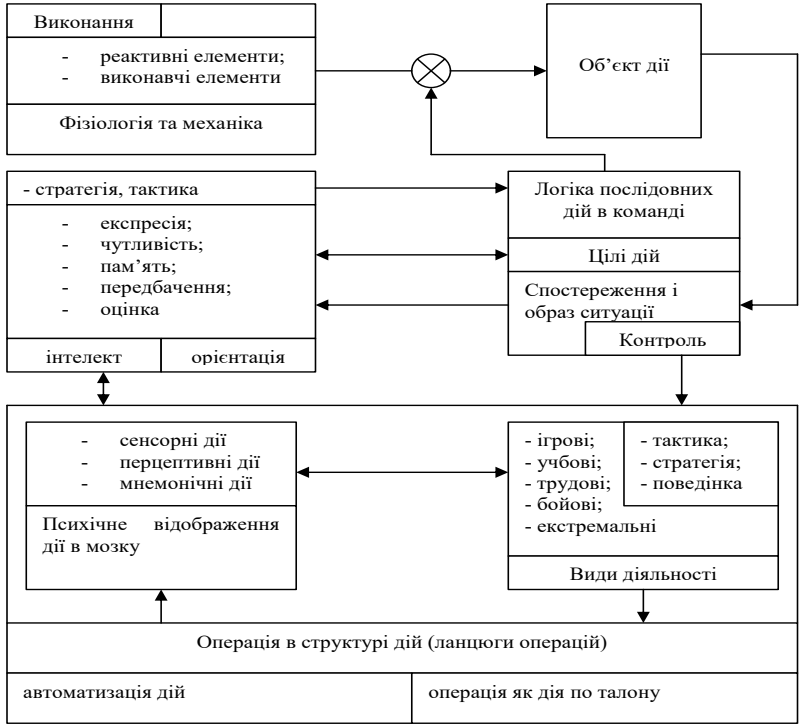


Рисунок 2 – Функціональна схема елементів інтелектуальної діяльності

3. Принципи функціонування систем з ієрархічною організаційною структурою:

– принцип ієрархії організаційної структури;

– принцип зворотного зв'язку в тріаді: стан об'єкта відносно цілі – корекція стратегії зміни стану відносно досягнення мети – дії (тактика) для досягнення мети – контроль ефекту дій при вибраних стратегіях поведінки;

– гарантоване досягнення мети, як стратегія цілеспрямованості системи.

Загальні принципи психології управління [1, 4–6] це: об'єктивність при дослідженні об'єкта; саморозвиток, як перетворення форм психічного відображення реальності в індивідуально-психологічні особливості та її характеристики; системність в аналізі взаємодії елемент-структура-особа-знання для реалізації цільових завдань; комплексність, як врахування в кожному складному явищі всіх факторів взаємодії елементів, підструктур, осіб; активність, як елемент інтелектуально-енергетичної взаємодії в грі з природою, системою, командою; принцип співвідношення повноваження ⇔ відповідальність за прийняті рішення і дії.

Методи психології управління в складних (людино-машинних) системах для оцінки інтелектуального рівня прийняття рішень. Метод дослідження – це спосіб, або шлях одержання необхідної інформації про явища та стан і структуру об'єкта, його динаміку в часі та просторі [1–4, 7].

Розглянемо основні методи дослідження поведінки:

– метод спостереження за об'єктом і ситуаціями;

– метод самоспостереження як процедура самоідентифікації відносно цільової задачі;

– метод опитування колективі та особи для формування психологічного та інтелектуального образу особи;

– метод експерименту, ґрунтується на теоретичних знаннях, цільових діях та процедурах і тестах для вияснення інтелектуального образу особи та оцінки психіки (розвиток, емоції, ціннісні орієнтації, активність, рівень конфліктності).

4. Рівень ієрархії діяльності особи як CIS (цілеорієнтована інформаційна система та схема аналізу діяльності особи. Діяльність – це система з інтелектуально-нейрофізичних і фізичних компонент: мотиви функціонального існування; цілі, які є основою зміни стану (дискомфорт); операції для досягнення цільового стану; дії, як спосіб реалізації системи операцій, які ведуть до досягнення мети.

Основною задачею психологічного аналізу діяльності особи є виявлення та пояснення причин і мотивів поведінки при досягненні мети (цільового стану). Ситуаційне спонукання особи до дій включає: генерацію цільової стратегії досягнення мети; виникнення цільової поведінки та її напрям; енергетичне забезпечення дій та оцінка їх наслідків; початок і закінчення дій на основі команд сформованих згідно стратегій реалізації цілі.

Особливості ситуації, які мотивують до діяльності: інтенсивність інформаційного впливу на особу; нестандартність образу ситуації; новизна стимулів до зміни стану; аварійні та кризові ситуації і загрози для існування особи; цільова стратегічна переорієнтація.

Процедури мислення [4], як відображення інтелекту особи: операційна функціональність; аналіз та генерація цвілевих гіпотез; абстрагування; порівняння; співставлення об'єктів при пошуку аналогій; виділення класів ознак; логічні операції побудови суджень; логічні операції побудови висновків; узагальнення; синтез – як процес об'єднання елементів в цілісну функціональну структуру.

Операція є динамічною виконавчою компонентою діяльності, як спосіб реалізації дії на основі інтелектуальної команди, яка входить в процедуру тактики досягнення мети. Операція є способом виконання дії і формується на основі автоматизації діяльності або наслідування поведінки еталонної системи, і є психічно мало усвідомлювана.

5. Концепція творчості при прийнятті рішень – креативність в умовах загроз. Творчість, як елемент інтелектуальної діяльності в цілеспрямованій системі CUS може проявлятися на різних етапах діяльності:

– постановка проблеми в умовах кризового стану і ризикованих ситуацій;

– зміна цілеорієнтації в умовах перевищення допустимого рівня загроз;

– ієрархічна перебудова структури бази знань і даних в напрямку пошуку засобів розв'язання виникаючих принципово нових проблем (специфічні мотиви, цілі, способи дії).

Творча діяльність становить базовий вимір багатоярусної інтелектуальної структури особи, яку доцільно диференціювати на такі головні компоненти діяльності – мотиваційний, цілеутворюючий, результативний, емоційно-чутливий, інформаційно-пізнавальний, генератор ідей (рис. 3). Творчість – це взаємодія, яка знаходиться в динамічному розвитку і механізм, якої має визначені фази функціонування [6].

Рисунок 3 – Ієрархічна схема багатоярусної інтелектуальної структури особи в процесах обробки інформативних даних

Фаза вільного логічного пошуку включає:

– актуалізацію знань необхідних для побудови процедури розв'язку проблеми;

– вибір процедури прийняття рішень на основі класифікації і кластеризації комплексу ознак; синтез стратегій досягнення цілі;

– перевірка можливості використання процедури прямого логічного виводу з наявних посилань (блоків знань), аналіз існуючих даних;

– узагальнення початкових знань;

– пошук аналогій розв'язку подібних проблем;

– перенесення відомих особі знань на нові умови, ситуації, проблеми;

– висунення гіпотез про спосіб класифікації альтернатив і моделей дерев та послідовностей, ланцюгів рішень.

Фаза інтуїтивного рішення виникає при таких етапах активізації підсвідомості людини (оператора): відсутності послідовності логічних дій адекватних стратегій розв'язання проблеми; неусвідомлений пошук способу рішення проблеми, в основі якого лежить принцип двоїстості результату дій особи (усвідомлений і неусвідомлений продукт дії) і його вплив та керуюча дія на послідовність дій.

Умови генерації регулюючих дій на процес пошуку розв'язку проблеми включають відповідні процедури, моделі, способи рішень: високий рівень пошукової мотивації; чітке формулювання задачі; відсутність автоматизації способу дій; нові способи досягнення цілі при неадекватності існуючих методів розв'язку проблеми, задачі, ситуації, що відповідно пов'язано з формуванням робастних стратегій досягнення мети.

Фаза вербалізації інтуїтивного рішення та логічне оформлення способу розв'язання нової задачі [7]. Інтуїтивне рішення проблеми на попередній стадії творчого процесу формується неусвідомлено. Усвідомлюється тільки результат, досягнутий в процесі рішення.

Основною особливістю творчої особи [6] є креативність, як інтегрована якість психіки людини, тобто можливості його інтелекту, який забезпечує продуктивне перетворення в ланцюгу процедур прийняття рішень, що ведуть до мети, на основі досліджувальної активності, яка характеризується наступними особливостями:

– *когнитивністю,* як високою сенсорною чутливістю до збурень і загроз, системним сприйняттям, аналітичною пам'яттю, образним мисленням і дивергентним стратегічним мисленням в процесі пошуку методів розв'язання певних класів задач;

– *емоційністю* при високому рівні збудження, управління станом особи в умовах загроз;

– *мотиваційністю і комунікативністю* в процесах прийняття рішення в умовах ризику і загроз.

Адаптація особи до зовнішньої ситуації та загроз виступає як процес активної взаємодії (організм ⇔середовище), що приводить до успіху в прийнятті цільових рішень на основі одержання нових знань в процесі дій.

В проблемних ситуаціях адаптація здійснюється за допомогою конструктивних механізмів в пізнавальних процесах, цілеутворенні, цілеорієнтації та ідентифікації поточних образів динамічного стану об'єкта взаємодії. Ці процеси є інформаційною основою формування стратегії прийняття цільових рішень (рис. 4).

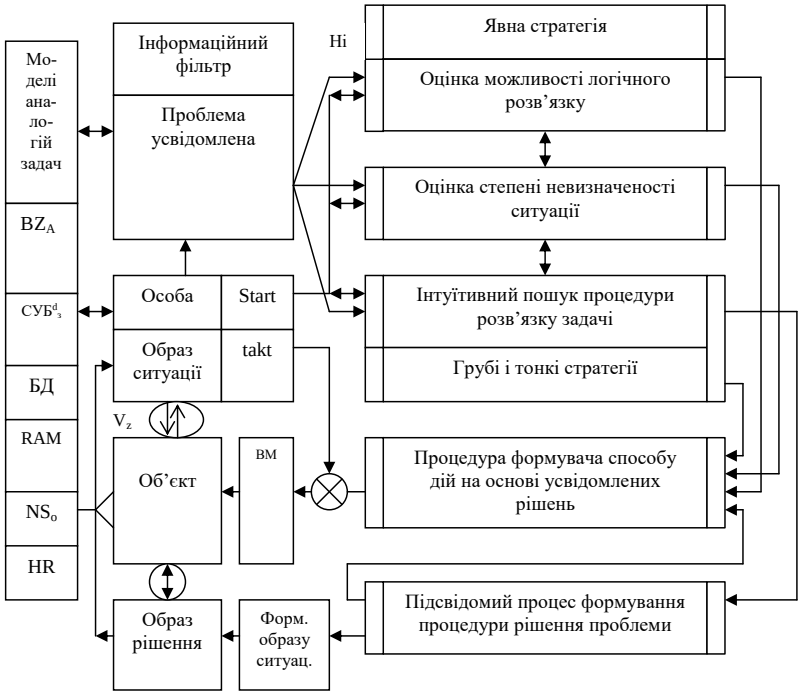


Рисунок 4 – Структурна схема процесів формування цільових рішень, де: BZA – база активних знань; СУБ – система управління; БД – база даних; RAM – оперативна пам'ять; HR – індикація ситуацій; Strat, takt – стратегія дій та їх тактика.

Висновки. Процеси розв'язання задач і проблем є основою підсвідомої та свідомої компонент інтелектуальної діяльності, а тому важливим є формування концепції ідентифікації механізмів розумової (інтелектуальної) діяльності особи.

Інформаційні джерела

1. Орбан-Лембрик Л. Є. Психологія управління. К.: Академвидав. 2003. 548 с.

2. Ткачук Р. Л., Ткачук Г. В., Сікора Л. С., Якимчук Б. Л. Інтелектуальна компонента, як складова формування моделі поведінки оператора. Моделювання та ін-

формаційні технології: Зб. наук. пр. – К.: ІПМЕ ім. Г. Є. Пухова НАН України, 2012. – Вип. 64. – С. 170–175.

3. Ткачук Р. Л., Сікора Л. С. Логіко-когнітивні моделі формування управлінських рішень інтегрованими системами в екстремальних умовах: посібник. Львів: Ліга–Прес, 2010. 404 с.

4. Дурняк Б. В., Сікора Л. С., Антоник М. С., Ткачук Р. Л. Когнітивні моделі формування стратегій оперативного управління інтегрованими ієрархічними структурами в умовах ризиків і конфліктів. Львів: Українська академія друкарства, 2013. 449 с.

5. Кузнєцов М. А., Заїка Є. В., Ходикіна Ю. Ю. Психологія моторної пам'яті: прикладні аспекти. Монографія. Харків: Діса Плюс, 2019. 446 с.

6. Михайличенко В. Є. Психологія розвиту особистості : Монографія. Х. : НТУ "ХПІ", 2015. 388 с.

7. Психологія / ред. Трофімов Ю. К.: Либідь. 2001. 552 с.

УДК 621.3

ІНТЕГРАЦІЯ ТЕХНОГЕННИХ ІЄРАРХІЧНИХ СИСТЕМ УПРАВЛІННЯ ПРИ ДІЇ ФАКТОРІВ ЗАГРОЗ

Любомир СІКОРА
Нестор ЯКИМЧУК
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *The concept of terminal situational space, procedures of integration and stratification of hierarchical control system on the interval of terminal time, is considered the article as it applies to energy and production.*

Keywords*: expert system, strategy, coordination, synthesis, hierarchy.*

Анотація. *На основі концепції Месаровича, в статті розглянуто та введено поняття термінального ситуаційного простору, процедури інтеграції і стратифікації ієрархічних систем управління на інтервалі термінального часу в приміненні до енергетики та виробництва.*

Ключові слова: *ієрархія, експертна система, інтеграція. страта, термінальне управління.*

Актуальність. Сучасний етап розвитку промислових структур характеризується їх виробничою, інформаційною, ресурсною інтеграцією на основі вироблення корпоративних стратегій, як основи реалізації глобальних цілей.

Прийняття рішень в таких структурах як в нормальних штатних, так і в надзвичайних ситуаціях є складною проблемною задачею, і тому для свого розв'язання вимагає необхідних інформаційних і системних технологій та логіко-математичних методів для побудови процедур і каналів рішень та моделей об'єктів і образів ситуацій в них [1, 2, 4].

Проблема опису динаміки об'єктів і систем. Моделі динаміки систем можна описати і представити (рис. 1, а) в фазовому просторі через координати (Rx_1, Rx_2) в базисі $(\vec{l}_1, \vec{l}_2, \varphi)$, де ($x_{10}$, x_{20}) – координати центру початкового стану $(x_1 \parallel l_1) \wedge (x_2 \parallel l_2)$, $\varphi = \omega t$ – фазовий кут пов'язаний з поточним часом $t \in T$, V_s – областю зміни ситуації $Sit\,D_S(t \in T) = F(Z, t \mid \varepsilon, U(C_i)), Z = x_1 + jx_2$, та областю аварійного режиму V_A^+.

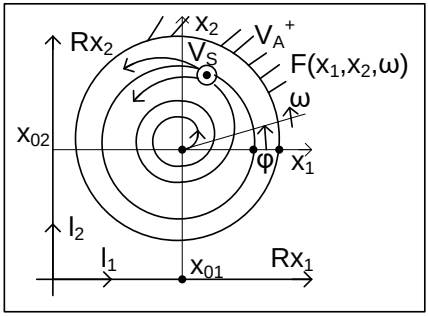
Поведінку потенційно небезпечного об'єкту (ПНО) вигідно представити в просторі станів $[R_\theta \times P_T]$ (рис. 1, б), як моделі траєкторії руху параметра стану, що відображається поточним розв'язком ДР-рівняння балансу ресурсів, при цьому виділяються області нормального стану $\left([\Theta_0^U + A\Theta, \Theta_0^U - A\Theta] \times R_t\right)$, області граничних режимів V_g^+, область зміни ситуації V_{S1}, V_{S2} в моменти часу t_1, t_2, які є координатами і з них починається формування і реалізація рішень управляючою системою, при цьому як ця процедура реалізовується в явній формі не видно [2].

Введення концепції цільового простору [2, 3] спряженого з простором станів, який грунтується на альтернативному розбитті простру стану по параметру $\Theta \in R_\theta$, $R_\theta = \bigcup_{i=1}^{n} \Theta_i = I_{\theta D}$ – з допустимим інтервалом станів $I_{\theta D}$ та термінальним часом $T_m \subset R_t, T_m \bigcup_{j=1}^{m} \tau_j$, дозволяє відслідковувати процес прийняття рішень на дискретних інтервалах часу при ручному або автоматизованому управлінні (рис. 1, в).

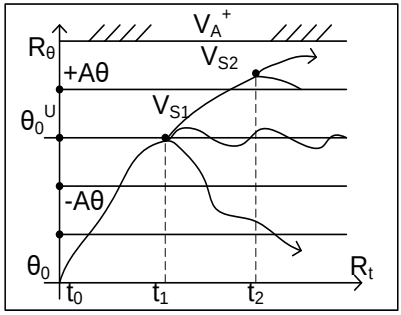
В умовах надзвичайних ситуацій, для оцінки ситуацій і термінів прийняття рішень важливим є момент й термін на процедуру формування та прийняття рішень для недопущення розвитку загроз. Тому на рівні оперативно-командного управління необхідно ввести поняття термінального ситуаційного простору який враховує термінальну структуру процесу формування і прийняття рішень. Ситуація описується через дерево зміни ситуативних станів D_S яке спроектоване в простір $[R_t \times R_T]$, де $R_T = \bigcup_{i=1}^{n} R_{Ti}$, $R_t = \bigcup_{j=1}^{m} \tau_{Rj}$ – утворюють розбиття на інтервалах реального і термінального часу (рис. 1, г).

Введення поняття термінального ситуаційного простору дозволяє виробити новий погляд на методику синтезу корпоративних стратегій управління на основі процедур ідентифікації ієрархії та розбиття ієрархічної структури на страти, як закінчені функціональні однорідні управляючо-виконавчі підсистеми. Це дозволяє врахувати для кожного рівня вимоги до надійності,

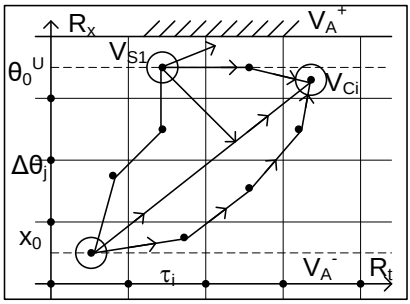
енергоресурсу, рівня запасу функціональної і конструктивної стійкості, рівня післяремонтного відновлення та запасу міцності, що є характерним для енергетичних систем, та складних хіміко-технологічних, нафтопереробних і транспортних систем.



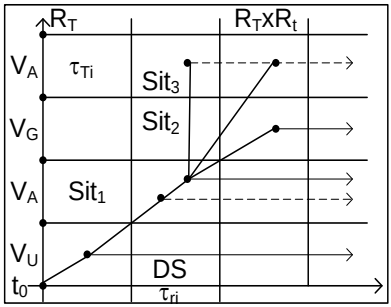
а) Фазовий простір



б) Простір станів



в) Цільовий простір



г) Термінальний ситуаційний

Рисунок 1 – Моделі образів ситуацій в інформаційно-ресурсних просторах станів ІІАСУ

Проведемо аналіз проблеми стратифікації. При цьому можемо виділити рівні страт:

– виробничі рівні;

– виробничо-управляючі рівні;

– інтелектуально-координуючі стратегічні рівні.

Стратифіковані організаційні ієрархічні системи та їх інтеграція в АСУ-ТП як основа координаційного управління будується на основі системного синтезу. Стратифікація пов’язана з трьома основними властивостями ієрархічних систем [1, 5]:

– вертикальною декомпозицією структури;

– ієрархією пріоритетів прийняття рішень і дій;

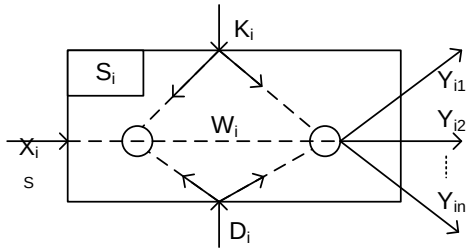
– взаємозв'язком характеристик якості функціонування всіх рівнів.

Стратифікація починається з чіткого виділення блоків вхідних даних, операторів функціональних перетворень і множини вихідних даних у вигляді:

$$\forall t \in T_m \subset R_t : \left\langle \mathrm{S}: \mathrm{X} \to \mathrm{Y}, \mathrm{X} = \overset{n}{\underset{i=1}{\otimes}} \mathrm{X_i}, \mathrm{Y} = \overset{n}{\underset{i=1}{\otimes}} Y_{\mathrm{i}}, i \in N_k \right\rangle$$

який визначає можливість розбиття вихідних і вхідних сигналів на компоненти. Тоді кожній S_i -страті можна приписати відповідно перетворення вхідних і координуючих сигналів у S_i -страті.

$$\begin{cases} i = n \Rightarrow S_i : X_{iS} \times W_i \to Y_i; \\ i < n \Rightarrow S_i : X_{iS} \times W_i \times K_i \to Y_i \\ i > 1 \Rightarrow S_i : X_{iS} \times W_i \times D_i \to Y_i \\ i > n \Rightarrow S_i : X_{iS} \times (K_i \otimes D_i) \to \end{cases}$$



де X_{iS} – вхідний сигнал *i*-страти; W_i – передавальна функція; K – координуючий сигнал з верхнього рівня; D_i – сигнал про стан нижньої страти. Або у вигляді структури стійкої страти зі зворотними зв'язками де S_i – основна структура страти; S_{i+1}^{*} – система зворотного зв'язку; h_{i1} – модель спостерігаючої підсистеми; $K[C_{i+1}]$ – модель координуючої компоненти для страти нижнього рівня.

Стратифікація як процедура системного аналізу, відповідно, групує і оцінює потоки даних які йдуть на верхній рівень ієрархії, за рахунок опрацювання вхідних сигналів від нижніх страт і керуючих сигналів свого рівня. Агрегування об'єктів управління дозволяє впорядковувати їх структури та розбити множину параметрів на класи: вхідні, вихідні, керуючі, збурюючі фактори.

Відповідно будується ієрархія задач які розв'язуються в кожній страті згідно списку $Spys\,[ZD_i]$ з використанням алгоритму T_{i}: $Alg[T] \to \Pi R_{rz}(U, Z_i)$ як процедури розв'язання задачі цільового управління.

Особливістю організаційної ієрархії є точне визначення взаємодії (правил) підсистем по вертикалі.

Структурні компоненти страт по Месаровичу [1] задані схемою (рис. 2).

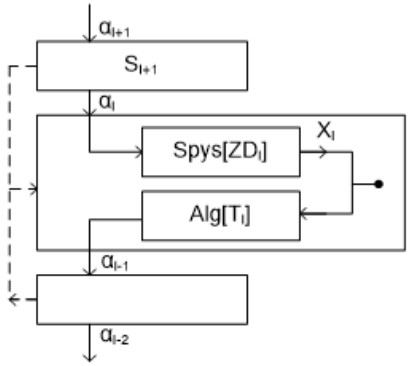


Рисунок 2 – Структурні компоненти страти

Для кожної структури можна провести процедуру декомпозиції процесу в об'єкті управління та процесу управління, як способу перетворення рішень задач.

Для структурованого процесу координаційного управління в страті маємо відповідне представлення:

$$H_i^U : M_i \times U_i \times \Omega_i \to Y_i,\ H_i^M : M \times Y \xrightarrow{\mu} U_i,\ H_k : (U_i^T, \Omega) \times M \to ,$$

де: U_i – множина вхідних управляючих сигналів; U_i^T – термінальне управління; M_i – множина вхідних сигналів стану об'єкту; $M_i \equiv \left\{S_i^m, S_{i+1}^m, S_{i-1}^m\right\}$, Ω_i – сигнал збурення; Н – проекційні відображення яке пов'язує підпростори станів процесу (фазового, стану об'єкта, цільового системи та термінального), Y_i – вихідний сигнал пов'язаний через U_i.

Дія збурень на процес представлена через К-оператор $K = \left\langle K^U, K^D \right\rangle$ де K^U – визначає вплив на управляючі команди, K^D – дезорієнтуючий вплив на системи контролю стану компонент страти. $K^U : M \times \Omega \to U$, або через $K^D : M \times \Omega \to Y_i$, відповідно маємо:

$$\hat{U}(m,\omega) = K(m,\omega) = H(m, P(m,\omega));$$

$$H^U(m,\omega) = P(m, K(m,\omega), \omega);$$

$$P_i(m,\omega) = M_i \times U_i \times \Omega_i \mid \forall \omega \in \Omega.$$

Наведемо базові компоненти функціональних підструктур *i*-страт в ієрархічній організаційно-виробничій системі (рис. 3).

На рисунку 3 де (1, 2, 5) – функціональні блоки; (3, 6) – керуючі блоки; (4, 7, 8) – рішаючі пристрої з виконавчими командними процесорами.

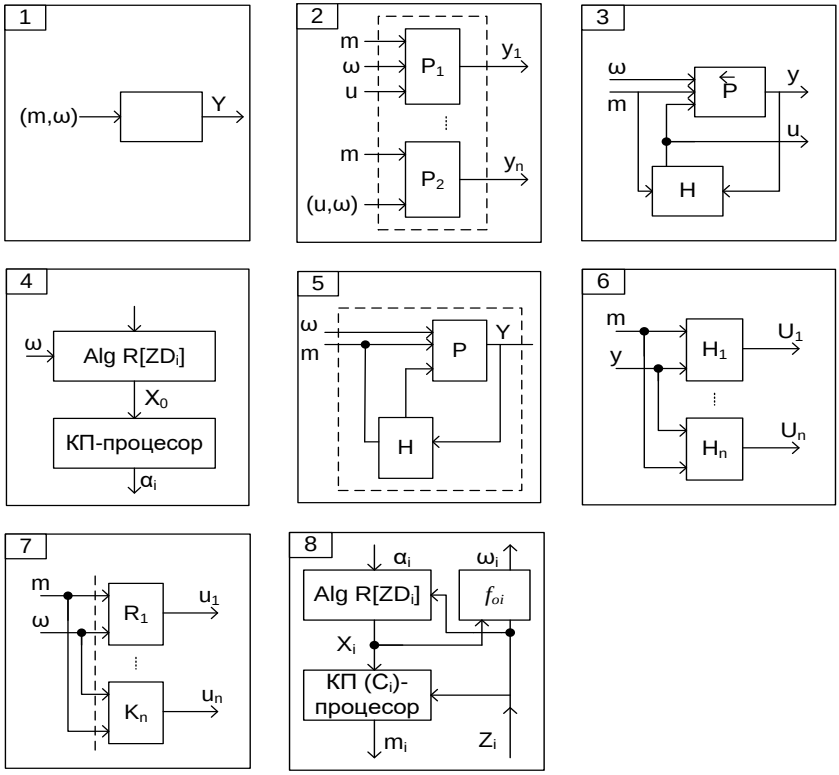


Рисунок 3 – Базові компоненти підструктур *i*-страт в ієрархії системи

Для реалізації координуючого управління формується n-рівнева ієрархія прийняття рішень яка має об'єктний рівень та *n*-2 рівнів локального управління і *n*-й рівень глобального управління. Відповідно будується схема ділового управління (рис. 4).

Для класичної теорії координацій Месаровича [1] основною проблемою є побудова оптимальних стратегій управління процесами на *n*-рівнях ієрархії з узгодженням локальних і глобальних цілей в нормальних режимах функціонування. Для управління в умовах НС в ПНО необхідна модернізація концепцій, оскільки управляючі дії носять термінальний характер, тобто на момент виникнення загрозливої ситуації необхідно:

– прийняти міри для їх попередження та ліквідації;

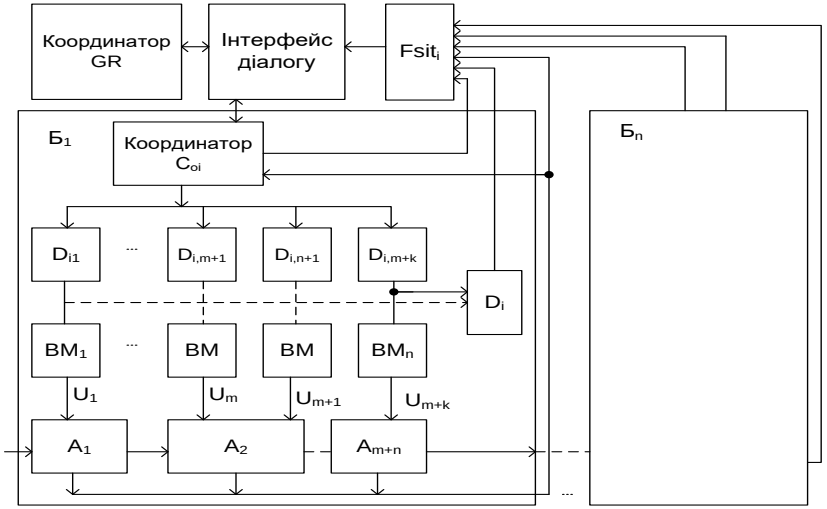


Рисунок 4 – Схема ділового управління з координатором в ієрархічній системі, де: $Fsit_i$ – формувач образу ситуації в момент t_i; C_{oi} – локальний координатор; D_{in} – підсистеми *i*-рівня прийняття рішень; ВН – виконавчі механізми; $\{A_i\}$ – агрегат об'єктного рівня, $Б_1 \ldots Б_n$ – базові компоненти виробничої структури.

– сформувати маршрути для каналів зв'язку з цільового діалогового і командного обміну інформацією на всіх рівнях ієрархії;

– виробити стратегію гнучкої координації і ієрархічній системі зі змінною структурою;

– визначити ключові механізми управління агрегатами;

– визначити координати механізмів ручного і автоматичного управління ресурсами агрегатів;

– визначити картографічні і навігаційні параметри об'єкта з потенційно-небезпечною енергоактивною структурою та його фізико-хімічну та енергетичну організацію;

– визначити маршрути руху оперативно-командних ліквідаційних груп, які забезпечать ліквідацію загроз на ПНО;

– сформувати ієрархію оперативно-командного управління з інтеграцією її в структуру системи управління ПНО на рівні всіх страт;

– синтезувати, на основі баз знань, координуючі стратегії та побудувати тактичні плани її реалізації на всіх рівнях ієрархії;

– виконати план дій по ліквідації загроз, згідно схем управління агрегатами для всіх базових компонент виробничої системи і ПНО.

Процедура стратифікації складної виробничої структури включає елементи інформаційних технологій та системний аналіз для виділення страт в її ієрархічній організації, методів теорії баз даних і знань для побудови системи підтримки прийняття рішень, технологій експертних знань для виявлення конструктивних можливостей і міцності елементів ПНО в яких можливе виникнення аварій за рахунок втрати механічних властивостей агрегатів.

Висновки. На основі теорії ієрархічних систем розглянуто моделі і підходи до стратифікації і інтеграції складних систем, обґрунтована концепція підвищення їх ефективності і функціональної надійності.

Інформаційні джерела

1. Сікора Л. С. Робастні та інформаційні концепції в процедурах синтезу систем управління : Держ. н.-д. ін-т інформац. інфраструктури НАН України, Інж. акад. України, Центр стратег. дослідж. еко-біотехн. систем. Л. : Центр стратегічних досліджень еко-біотехнічних систем, 2001. 578 с.

2. Сікора Л. С. Системологія прийняття рішень на управління в складних технологічних структурах. Львів: Каменяр, 1998. 453 с.

3. Дурняк Б. В., Сікора Л. С., Антоник М. С., Ткачук Р. Л. Когнітивні моделі формування стратегій оперативного управління інтегрованими ієрархічними структурами в умовах ризиків і конфліктів. Львів: Українська академія друкарства, 2013. 449 с.

4. Ткачук Р. Л., Сікора Л. С. Логіко-когнітивні моделі формування управлінських рішень інтегрованими системами в екстремальних умовах: посіб. Львів: Ліга–Прес, 2010. 404 с.

5. Дурняк Б. В., Сікора Л. С., Антоник М. С., Ткачук Р. Л. Автоматизовані людино-машинні системи управління інтегрованими ієрархічними організаційними та виробничими структурами в умовах ризику і конфліктів. Львів: Українська академія друкарства, 2013. 514 с.

УДК 621.3

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ СТВОРЕННЯ СЦЕНАРІЇВ ДІАЛОГУ ДЛЯ УПРАВЛІННЯ В ІЄРАРХІЇ АСУ-ТП ІНФРАСТРУКТУРИ

***Богдана ФЕДИНА*[1, 2]**
***Юрій ЛИСИЙ*[1]**
***Роман СИДОРЕНКО*[1]**

[1]Національний університет "Львівська політехніка", м. Львів, Україна.
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.

Abstract. *On the basis of information technologies of the systems of support of making decision and hybrid intellect going is considered near the construction of scenarios of development of events in the management automated information.*

Keywords: *dialogue, scenario, hybrid intelligence, system, content.*

Анотація. *На основі інформаційних технологій систем автоматизованого проектування та гібридного інтелекту розглянуто підходи до побудови сценаріїв розвитку подій в інтелектуальних автоматизованих системах управління технологічними процесами.*

Ключові слова: *діалог, сценарій, гібридний інтелект, система, зміст.*

Зростання інтенсивності виробничих процесів в технологічних системах створює ряд проблем контролю і управління в ієрархічних системах (ІС), а саме:

– підняття рівня психологічного навантаження через неадекватність засобів відображення ситуації на потенційно-небезпечних аспектах (ПНО) технологічних систем для операторів нижнього рівня ІС;

– нездатність сприймати зміст ситуації та прогнозувати сценарій розвитку подій та будувати плани попереджуючих дій;

– зниження рівня гарантій функціонування ПНО за можливих переходів параметрів конструкцій за межі міцності;

– невизначеність оцінки ситуації за рахунок часткової або повної втрати технологічної документації, що приводить до некоректної інтерпретації розвитку подій;

– низький інформаційних рівень відображення даних (затримки і збої, спотворення, блокування, несправність вимірювальних систем) що приводить до неправильного трактування режимів функціонування ПНО-ІС;

– відсутність мультимедійного багатоканального інтерпретатора динаміки розвитку подій.

Перелічені вище положення, щодо інформаційного та інтелектуального опрацювання та відображення потоків подій підтверджує актуальність проблеми створення систем діалогу в ІС та синтезу процедур побудови сценаріїв в розвитку подій [1, 3, 4].

Сценарій діалогу – це детальний опис структури та змісту діалогу. Він є найбільш повним відображенням структури діалогу. Явне виділення структури діалогу через сценарій дозволяє контролювати допустимі послідовності станів, локалізувати зміни в структурі діалогу, спростити розробку і налагодження програм [1, 2]. Сценарій діалогу включає в себе інформаційну та операційну моделі й у формальному вигляді задається:

$Scen[Dialog(R_A \leftrightarrow S)]: <S_i, A, C, R_V, G, I, \Omega>$

де S – система, S_i – стани ($i \in N$), A – множина операцій, $C=(Q \cup F)$ – множина умов, Q – множина вхідних повідомлень, R_V – множина вхідних умов, R_A – оператор, $G \equiv (S_i \times C)$ – структура графу діалогу.

Відповідно представлення інформаційної моделі діалогу має вид:

$$I_M[\text{Dialog}(R_A \leftrightarrow S)]: \begin{vmatrix} S_i \rightarrow R_V \\ (S_i \times C|_{i \in N}) \rightarrow R_V \end{vmatrix};$$

а операційна модель має вид:

$$\Omega_M^A[\text{Dialog}(R_A \leftrightarrow S)]: \begin{vmatrix} S_i \to A \\ (S_i \times C\,|_{i\in N}) \to A \end{vmatrix}.$$

Схема побудови сценарію діалогу наведена на рисунку 1.

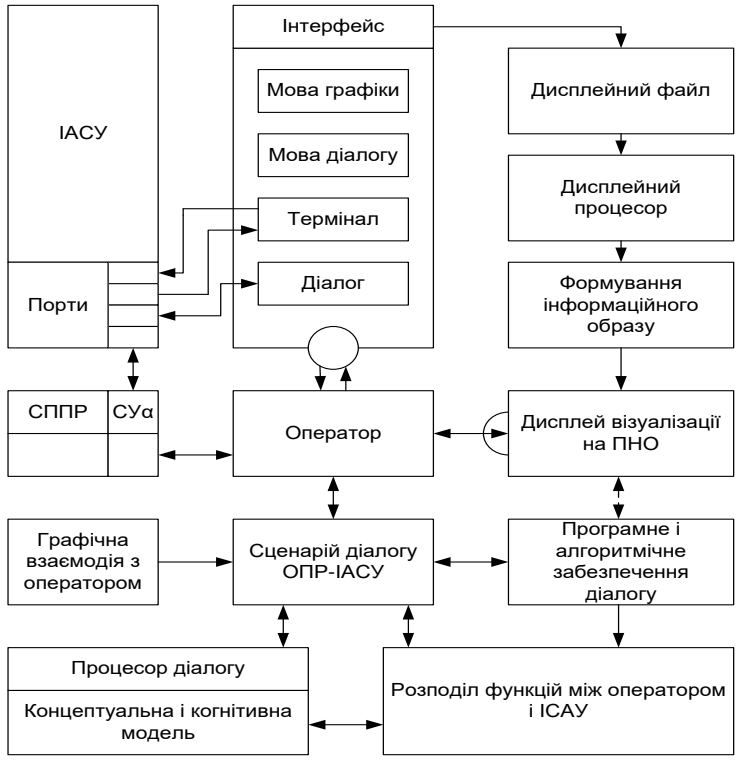


Рисунок 1 – Схема побудови сценарію діалогу

Автоматичне ведення діалогу, згідно сценарію, визначається програмно-логічною його інтерпретацією. Основою інтерпретації служать наступні управляючі конструкції: діалогове повторення; діалогове розгалуження; діалоговий мультицикл. Ці елементарні діалогові управляючі конструкції називаються вузлами сценарію. Інтерпретатор в кожному вузлі сценарію виконує наступні функції: видача повідомлення про поточний стан; ввід запиту користувача; аналіз умов, виконання умовних операцій; перехід до наступного стану по графу діалогу. Наведемо схеми діалогових управляючих конструкцій (рис. 2).

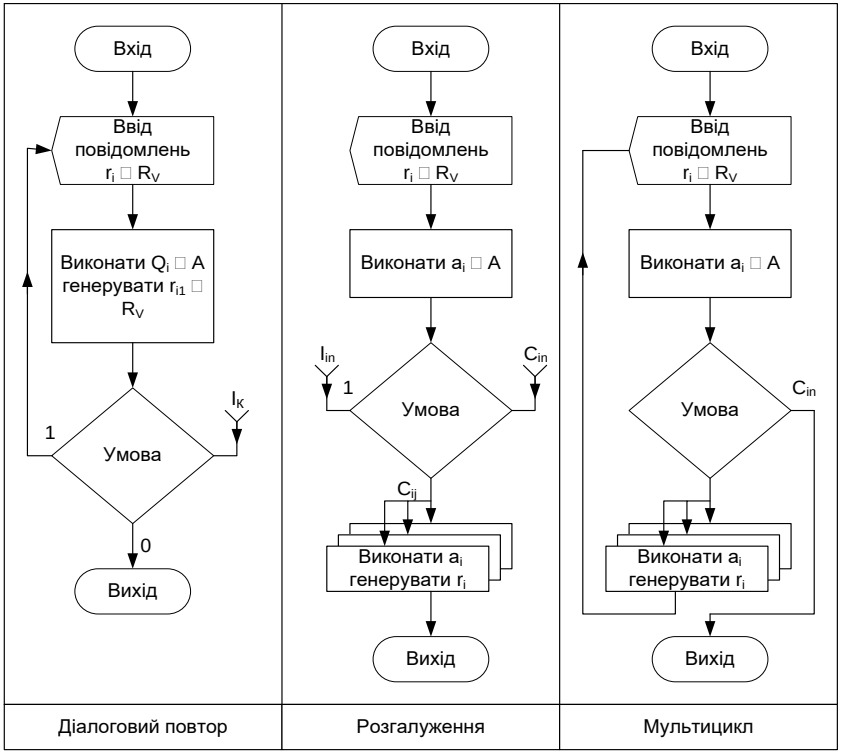


Рисунок 2 – Схеми діалогових управляючих конструкцій

Призначення діалогу в інтелектуальних автоматизованих системах управління технологічними процесами (*ІАСУ-ТП*). Основним цільовим призначенням діалогу є сумісне розв'язання задач управління в *ІАСУ*. При цьому маємо два аспекти діалогової взаємодії [2, 4, 6]:

– *інформаційний* – пов'язаний з обміном потоками даних про ситуацію і стан ПНО;

– *координаційний* – забезпечує координацію управляючих дій учасників діалогу.

Метадіалог як основа декомпозиції структури діалогу виконує наступні функції:

– організацію сеансу діалогу;

– переривання сеансу;

– зміна форми діалогу;

– ввід-вивід на термінал;

– процедура перегляду кадрів діалогу;

– видача інструкцій і допомоги;

– управління послідовністю кроків рішення задач (ходом обчислювального процесу);

– комбінація і розподіл функцій;

– зв'язок між користувачами системи;

– забезпечення об'єктно-орієнтованого діалогу.

Діалогові засоби апаратно-програмного забезпечення включають наступне:

– операційні системи;

– пакети прикладних програм;

– пакети драйверів управління терміналом вводу і виводу даних;

– драйвери моніторів візуалізації;

– діалогові редактори текстів та ін.

Сценарна організація діалогу. Процедурна реалізація діалогу ґрунтується на використанні операторів діалогових мов програмування, також підпрограм термінального вводу-виводу.

Способи реалізації сценаріїв. Основними рисами реалізації сценаріїв є:

– формальний логіко-математичний апарат опису сценаріїв;

– спосіб опису сценарію діалогу;

– форма і структура діалогу (інформаційна, логічна, системна);

– структура вузла сценарію діалогу;

– можливість мультимедійного вкладеного опису сценарію;

– спосіб зберігання і формат сценарію;

– засоби забезпечення діалогу;

– створення протоколу станів діалогу;

– організація прикладної діалогової програми.

В якості формального апарату для побудови структури сценаріїв діалогу використовуються:

– теорія графів;

– теорія автоматів;

– теорія формальних граматик;

– сітки Петрі;

– теорія ігор та системний аналіз.

В інтерпретуючому варіанті сценарію, його опис зберігається на зовнішньому носії у вигляді символьного файлу або завантажувального модуля. Використовується також інтерпретація сценаріїв через процедурні мови у вигляді фреймів. Виконавчі оператори фреймів мають наступне призначення:

– виконання діалогового обміну;

– виклик підпрограми;

– виконання умовного та безумовного переходів;

– виконання управляючих конструкцій (розгалуження, вибір, цикл);

– передача управління іншому фрейму;

– виклик фрейма з поворотом;

– повернення управління фрейму.

Відповідно, структура сценарію діалогу має наступний вигляд (рис. 3).

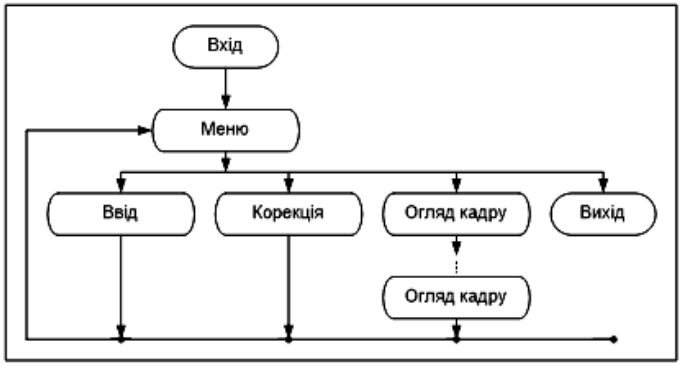


Рисунок 3 – Структура сценарію діалогу

Розглянемо алгоритм інтерпретації сценарію, який включає наступні кроки [1, 3, 7]:

– на початку циклу інтерпретації зчитується опис наступного циклу сценарію;

– виконується макетний обмін з контролем і перетворенням даних;

– виконується ланцюг безумовних переходів в підпрограмах опрацювання блоків даних;

– виконуються, після аналізу результатів обробки даних, умовні переходи;

– виконується циклічний перехід;

– виконується перехід на новий пункт сценарію.

Програмне забезпечення діалогу складається з інструментальних, апаратних і системних засобів організації діалогу, операційної системи діалогу реального часу [2, 5].

Інформаційне забезпечення діалогу включає [3]:

– представлення мультимедійних кадрів;

– система підказок;

– каталог тем і повідомлень;

– каталог сценаріїв;

– контрольні точки;

– каталог користувача.

Діалоговий інтерфейс призначений для підтримки передачі даних між терміналом та процесорним і моніторним програмно-апаратним забезпеченням [3, 7]. На рисунку 4 наведено схему алгоритму інтерпретації сценарію.

Склад пакету програмного забезпечення (ППЗ) включає:

– системне ядро пакета програм (ПП);

– інструментальні засоби діалогу;
– технічні та технологічні засоби діалогу;
– дисплейні комплекси.

Системне ядро пакету програм забезпечує запуск і завершення роботи діалогової мультимедійної підсистеми, ініціювання процесів користувача, ведення зовнішнього діалогу, завантаження пакету програм.

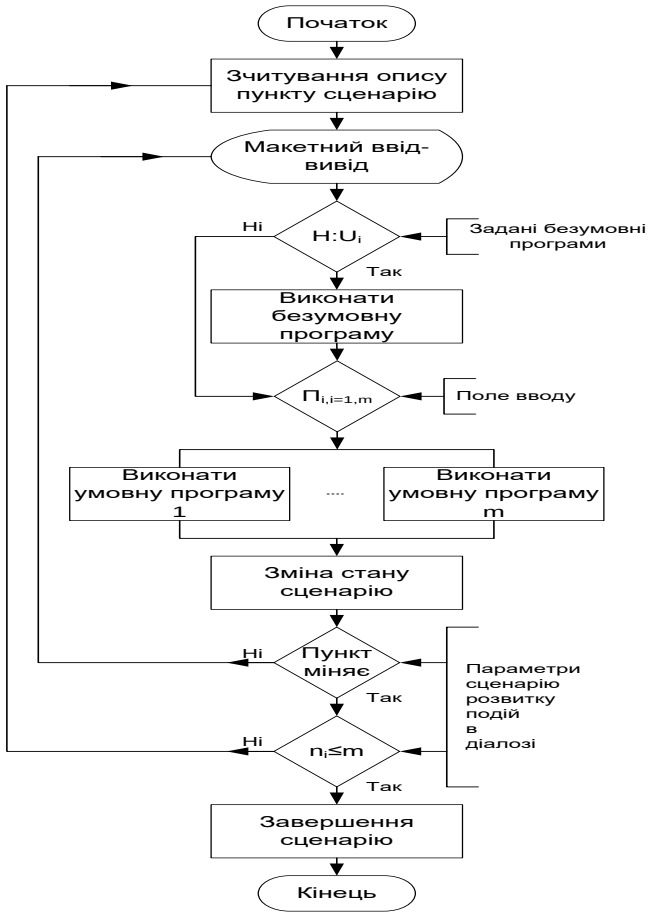


Рисунок 4 – Алгоритм інтерпретації табличного сценарію

Інструментальні засоби діалогу – це набір процедур вбудованих в пакет програм діалогу, які забезпечують організацію внутрішнього діалогу, редагування тексту, бібліотечні функції в діалоговому режимі, запуск пакетів завдань.

Технологічні засоби діалогу призначені для підготовки сценаріїв та кадрів діалогу, генерації діалогових програм, реєстрації нових мультимедійних сцен. Сукупність файлів і апаратно-програмних засобів утворють інформаційне середовище діалогу (рис. 4).

Усі файли можна розділити відповідно на: системні (каталог тем діалогу, облік користувачів, бібліотека сценаріїв діалогу, файл кадрів, бібліотека завантажувальних модулів функціонального ППЗ, файли редагування) та на користувацькі файли (файли баз даних, ППЗ).

Сукупність файлів, ППЗ, пристроїв відбору і опрацювання даних, відображення ситуацій на екрані дисплеїв (карти, образи, графічні кадри) утворюють інформаційне середовище, в якому можна виділити – системні і користувацькі файли.

Висновки. На основі інформаційних технологій, моделей гібридного інтелекту та когнітивної психології, в праці розглянуто підходи для створення інформаційної моделі сценарію діалогу в ІАСУ, що дає змогу підняти рівень оперативного управління в нормальних та екстремальних ситуаціях.

Інформаційні джерела

1. Дурняк Б. В., Сікора Л. С., Антоник М. С., Ткачук Р. Л. Когнітивні моделі формування стратегій оперативного управління інтегрованими ієрархічними структурами в умовах ризиків і конфліктів. Львів: Українська академія друкарства, 2013. 449 с.

2. Сікора Л. С. Когнітивні моделі та логіка оперативного управління в ієрархічних інтегрованих системах в умовах ризику. Львів: ЦСД, 2009. 432 с.

3. Ткачук Р. Л., Сікора Л. С. Логіко-когнітивні моделі формування управлінських рішень інтегрованими системами в екстремальних умовах: посіб. Львів: Ліга–Прес, 2010. 404 с.

4. Дурняк Б. В., Сікора Л. С., Антоник М. С., Ткачук Р. Л. Автоматизовані людино-машинні системи управління інтегрованими ієрархічними організаційними та виробничими структурами в умовах ризику і конфліктів. Львів: Українська академія друкарства, 2013. 514 с.

5. Лиса Н. К., Сікора Л. С., Ткачук Р. Л., Тупичак Л. Л., Таланчук Р. Р., Федина Б. І., Федевич О. Ю. Інформаційні та когнітивні технології оцінки ситуації в автоматизованих системах управління в умовах дії завад і факторів збою. Комп'ютерні технології друкарства. 2020. № 1 (45). – С. 110–130. doi: 10.32403/2411-9210-2021-1-45-110-130. URL: https://ctp.uad.edu.ua/images//ktd/45_11.pdf

6. Sikora L., Lysa N., Tkachuk R., Fedyna B., Fedevich O. Information and Cognitive Components of Knowledge Formation in Procedures for Assessing Dynamic Situations in Cyber-Physical // CEUR Workshop Proceedings. – 2022. – Vol. 3156 : proceedings of the 3rd International workshop on intelligent information technologies & systems of information security, Khmelnytskyi, Ukraine, March 23–25, 2022. pp. 129–139. ISSN1613-0073. (SciVerse Scopus). URL: https://ceur-ws.org/Vol-3156/paper7.pdf

7. Сікора Л. С., Лиса Н. К., Ткачук Р. Л., Федина Б. І., Кунченко-Харченко В. І. Інтеграція ігрових, системних та інформаційно-ресурсних концепцій оцінки енергоактивної взаємодії техногенних і екологічних систем (Ч. 2). Науковий вісник НЛТУ. 2019, т. 29, № 1. – С. 126–135. URL: https://doi.org/10.15421/4029012

УДК 004.94:681

ВІДМОВОСТІЙКІСТЬ ЯК КРИТЕРІЙ ЯКОСТІ ВЕБЗАСТОСУНКУ

Ірина ПІХ
Соломія БРАТАШ
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *Failure prediction and localization methods to improve the fault tolerance of web applications have been investigated and optimized. Ensemble learning was used for predicting failure times, and principal component analysis (PCA) was used for anomaly localization. This improved the accuracy of failure detection and reduced system recovery time. A comprehensive approach was developed that integrates multiple analysis methods and data sources to enhance the stability and reliability of web applications.*

Keywords*: fault tolerance, failure prediction, ensemble learning, anomaly localization, web applications, PCA.*

Анотація. *Досліджено та оптимізовано методи прогнозування та локалізації збоїв для підвищення відмовостійкості веб-застосунків. Використано ансамблеве навчання для прогнозування часів відмов та аналіз основних компонент (PCA) для локалізації аномалій. Це дозволило підвищити точність виявлення збоїв та скоротити час відновлення системи. Розроблено комплексний підхід, що об'єднує кілька методів аналізу та джерел даних для покращення стабільності та надійності веб-застосунків.*

Ключові слова*: відмовостійкість, прогнозування збоїв, ансамблеве навчання, локалізація аномалій, веб-застосунки, PCA.*

Врахування критерію відмовостійкості під час веб-розробки є важливим завданням, оскільки саме надійність та стабільність роботи веб-застосунків визначає задоволення користувачів та ефективність бізнес-процесів.

Одним з основних викликів є забезпечення здатності системи автоматично відновлюватися після збоїв та підтримувати стабільну роботу в умовах динамічного навантаження. Існує потреба в ефективних механізмах для обробки помилок, таких як балансування навантаження, перенесення незавершених завдань на альтернативні ресурси та інформування про проблеми. Більшість наукових робіт з балансування навантаження (DLB) зосереджено на оптимізації таких метрик, як ресурсна ємність, використання ресурсів, рівень відмов, вартість ресурсів, критерії вибору ресурсів, аналіз черг, контроль дедлайнів та відновлення. Через динамічний характер середовища, відмовостійкість є важливим критерієм для розподілених та багатопотокових застосунків. Невиконані завдання передаються іншим придатним ресурсам для завершення виконання [1].

Відмовостійкість веб-застосунків є критичним фактором їхньої якості, оскільки сучасні системи повинні підтримувати роботу навіть при високих навантаженнях та непередбачених збоях. Одним із ключових підходів є прогнозування та своєчасне запобігання можливим відмовам, що є важливим завданням для забезпечення безперервності роботи веб-застосунку.

Незважаючи на значні обсяги досліджень методів відмовостійкості, існує не так багато рішень, що стосуються напрямку прогнозування проблем, особливо у великих системах, таких як ті, що використовуються у високопродуктивних обчисленнях (HPC).

Метою прогнозування збоїв є автоматичний аналіз даних, зібраних різними моніторинговими інструментами, та подальша передача здобутої інформації інструментам відмовостійкості для швидкого відновлення після відмов або своєчасного запобігання багам [2].

Важливим елементом є аналіз великих обсягів даних, отриманих від різних компонент системи, з метою ідентифікації шаблонів збоїв. Це складне завдання, оскільки "шаблони збоїв" і їх першопричини часто приховані у величезних обсягах інформації.

За допомогою поєднання та взаємної кореляції даних з різних джерел, ми прагнемо вловити різноманітні шаблони відмов та взаємодії в системі, навіть коли ці шаблони динамічно змінюються з часом. Поєднання та координація кількох методів прогнозування, має на меті підвищення покриття та точності прогнозування [2].

Щоб вирішити проблему, пропонується об'єднати два підходи. Один полягає в інтеграції кількох джерел даних, а інший полягає в поєднанні різних методів редагування (включаючи статистичне навчання, інтелектуальний аналіз даних або розпізнавання шаблонів). Тобто робота зосереджена на пошуку відповіді на два запитання. Перше – це питання "коли", тобто передбачити, момент виникнення ймовірних збоїв. Друге – це питання "де", тобто визначити, в якій частині системи ймовірно виникнуть збої.

Щоб відповісти на запитання "коли", ми розробили механізм прогнозування на основі ансамблевого навчання (рис. 1). Оскільки необроблені дані, зібрані різними інструментами моніторингу, часто мають різні формати та містять повторювані або зайві записи, на етапі попередньої обробки подій необроблені дані очищаються та класифікуються. Цей крок призначений для отримання унікального стандартизованого набору подій.

Через недостатність інформації в журналі RAS, прогнозування на основі ансамблевого навчання може лише виявити, коли система поводиться ненормально, без виявлення першопричини (тобто компонент, які викликають проблему). Щоб відповісти на запитання "де", розроблено метод локалізації на основі PCA (аналіз основних компонент):

$$X_{(mxk)xn} \rightarrow Y_{pxn} \rightarrow Anomaly \qquad (1)$$

Локалізація аномалій на основі PCA складається з таких кроків:

1) $X_{(mxk)xn}$ – збір початкових даних;

2) $X_{(mxk)xn} \rightarrow Y_{pxn}$ – видобуток характеристик;

3) $Y_{pxn} \rightarrow Anomaly$ – виявлення відхилень.

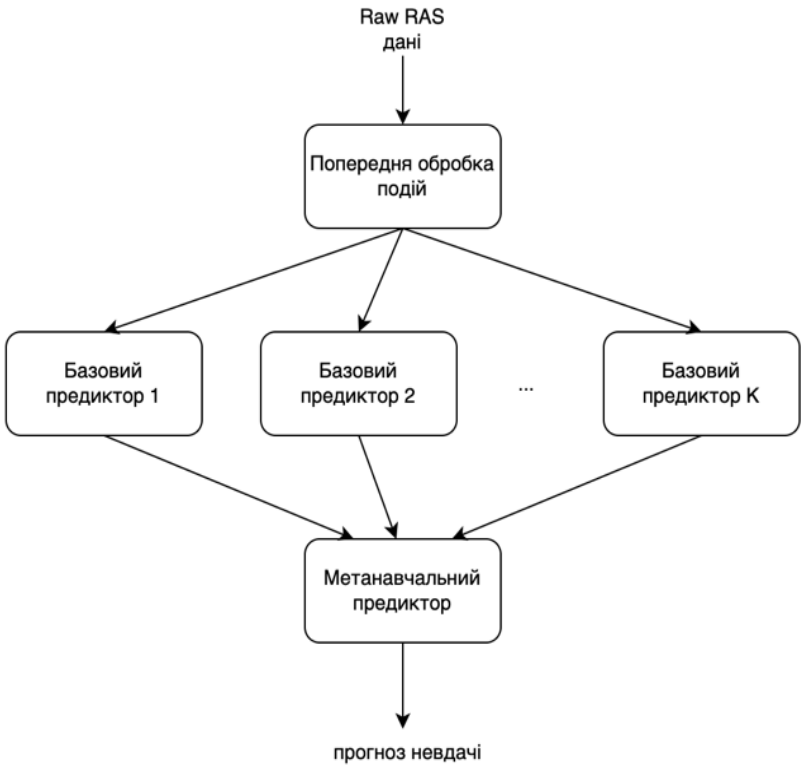


Рисунок 1 – Прогнозування на основі ансамблевого навчання

Кожен вузол збирає матрицю характеристик X^i розмірності mxk, де

$$X^i = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1k} \\ x_{21} & x_{22} & \cdots & x_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mk} \end{bmatrix} \quad (2)$$

PCA є добре відомою технікою розпізнавання образів, яка успішно використовується в багатьох областях для зменшення розмірності даних [3].

Отже, розробка відмовостійких веб-застосунків вимагає комплексного підходу, що поєднує як методи для швидкого відновлення після збоїв, так і прогресивні методи прогнозування відмов. Це дозволяє значно знизити ризики втрат даних, підвищити стабільність роботи та якість обслуговування користувачів.

Результати. В результаті дослідження методів прогнозування та локалізації проблем для підвищення відмовостійкості веб-застосунків було проведено оцінку за допомогою трасових досліджень та ін'єкцій збоїв. У дослідженні від SDSC та ANL, механізм прогнозування на основі ансамблевого навчання продемонстрував здатність виявляти понад 65% відмов, при цьому рівень хибних спрацьовувань залишався меншим за 35%.

Тобто, як точність *(Precision)*, так і повнота *(Recall)* перевищили 65%. Зокрема, точність визначалась як:

$$\Pr ecision = \frac{T_p}{T_p + F_p} \qquad (3)$$

де T_p – кількість правильних прогнозів (істинно позитивні), а F_p – кількість хибних спрацьовувань (помилково позитивних). В той час повнота (Recall) визначалась як:

$$\mathrm{Re}\, call = \frac{T_p}{T_p + F_n} \qquad (4)$$

де F_n – кількість помилкових непередбачених відмов (помилково негативні).

Наведені результати свідчать про високі показники ефективності прогнозування, оскільки значення Precision та Recall знаходяться на рівні понад 65% [2]. Це означає, що механізм прогнозування здатний ефективно виявляти збої при порівняно низькому рівні хибних спрацьовувань, що важливо для підтримки відмовостійкості.

Висновки. Відмовостійкість є одним із ключових критеріїв якості веб-застосунків, що забезпечує надійність, ефективність та зручність для користувачів. Впровадження практик, які підвищують відмовостійкість, допомагає уникнути непередбачених простоїв та втрати даних, забезпечуючи стабільність роботи застосунків навіть у складних ситуаціях. Завдяки цьому, компанії можуть не лише зміцнити довіру своїх клієнтів, але й отримати конкурентну перевагу на ринку. У сучасному цифровому середовищі інвестування в відмовостійкість – це стратегічний крок, що сприяє довгостроковому успіху бізнесу.

Інформаційні джерела

1. Anju Shukla, Shishir Kumar & Harikesh Singh, "Fault tolerance based load balancing approach for web resources", Journal of the Chinese Institute of Engineers, 2019.

2. Zhiling Lan, Yawei Li, Ziming Zheng, and Prashasta Gujrati. "Enhancing Application Robustness through Adaptive Fault Tolerance", International Symposium on Parallel and Distributed Processing, 2008.

3. Duda R., Hart P., and Stork D., "Pattern Classification". Wiley Interscience, New York, NY, 2nd edition, 2001.

УДК 004.056

КОНЦЕПЦІЯ САМОСУВЕРЕННОЇ ІДЕНТИЧНОСТІ ЯК АЛЬТЕРНАТИВА ТРАДИЦІЙНИМ МЕТОДАМ АВТЕНТИФІКАЦІЇ

***Василь ПОБЕРЕЖНИК*[1]**
***Валерія БАЛАЦЬКА*[2]**
***Іван ОПІРСЬКИЙ*[1]**

[1]Кафедра захисту інформації Національного Університету "Львівська Політехніка", м. Львів, Україна.

[2]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The concept of introducing a self-sovereign identity for personal authentication as an alternative to traditional user authentication methods, using a combination of blockchain technology and smart contracts to create a decentralized digital identity, and imposing a qualified electronic signature as a method of establishing identity belonging to a specific person is described.*

Keywords: *blockchain, smart contracts, digital identity, identification, digital signature.*

Анотація. *Описано концепцію впровадження самосуверенної ідентичності для автентифікації особи, як альтернативу традиційним способам автентифікації користувачів, застосування поєднання технології блокчейн та смарт-контрактів для створення децентралізованої цифрової ідентичності та накладання кваліфікованого електронного підпису як методу встановлення належності ідентичності конкретній особі.*

Ключові слова: *блокчейн, смарт-контракти, цифрова ідентичність, ідентифікація, цифровий підпис.*

Технології SSO (OAuth2, JWT) вирішують проблему повторної автентифікації користувачів на різних платформах шляхом автентифікації користувача через єдиний ідентифікатор. Однак, ці технології мають спільний недолік: сервер автентифікації, який є центральною точною вразливості, оскільки він відповідає за обробку інформації, яка пов'язана із автентифікацією користувача [1], тому вихід з ладу цього сервера спричинить відмову всієї системи. Також, потрібно зважати на те, що викрадення токену авторизації може призвести до несанкціонованого доступу до всієї системи.

Ще одним можливим способом автентифікації є система BankID [2, 3], яка надає можливість автентифікувати користувача та надати йому доступ до державних послуг, через використання банківських даних особи. Втім, в неї теж наявний недолік центральної точки вразливості, *наприклад*, збої у роботі через високе навантаження [4].

Шляхом вирішення проблеми центральної точки вразливості може стати застосування самосуверенної ідентичності [5], яка основана на застосуванні технології блокчейн.

Блокчейн – це децентралізована система, яка складається із блоків даних, які пов'язані в один ланцюжок за допомогою криптографії, та забезпечує збереження даних транзакцій у незмінному та прозорому вигляді. Криптогрфічним елементом, який зв'язує блоки є геш блоків, який дозволяє перевірити цілісність та достовірність блоку, а його збереження у наступному блоці дозволяє утворити стійкий зв'язок, який унеможливлює несанкціоновані зміни в системі [6]. Отже, ці властивості технології дозволяють розглядати її, як своєрідну основу для захищеної бази даних, яка може стати основою для створення цифрових ідентичностей, які забезпечуватимуть доступ до державних послуг.

Однак застосування лише самого блокчейну є недоцільним, через високі витрати ресурсів для зміни даних у блокчейні [7]. Тому доцільним є застосування технології смарт-контрактів. Загалом, смарт-контракти – це код, який сам себе виконує та існує у мережі блокчейн, а також надає можливість редагувати дані, які містять в ньому [8]. Тому застосування цієї технології дозволить забезпечити можливість зміни персональних даних за необхідності, а також описати процес взаємодії із цими даними, *наприклад*, автоматичне логування зміни даних, запиту на зчитування, чи, навіть, видалення даних з мережі. Отже, застосування смарт-контрактів дозволить не лише мінімізувати людський фактор із системи, але й забезпечить необхідний функціонал для оновлення облікових даних, при наявності такої потреби.

Основною особливості такого поєднання є те, що смарт-контракт можна прив'язати до криптогаманця особи, що дозволить їй бути власником облікових даних, відстежувати дії з даними та керувати дозволами на доступ до них [9]. Такий підхід дозволяє розглядати дану концепцію, як самосуверенну цифрову ідентичність, оскільки вона відходить від парадигми централізованої цифрової ідентичності, де управлінням даними ідентифікації займається певна установа чи сервіс.

Важливим елементом у такому підході залишається визначення створеного смарт-контракту, як ідентичності конкретної особи. *Наприклад*, в системі BankID це відбувається через багатофакторну автентифікацію на основі наявних банківських даних [3], втім такого підходу можна уникнути, якщо використати уже наявні механізми ідентифікації, *наприклад*, накладання цифрового підпису ДіЯ, який дозволяє ідентифікувати особу [10]. Такий підхід дозволить інтегрувати самосуверенні ідентичності в сферу державних послуг, що дозволить знизити навантаження на систему автентифікації користувачів, оскільки наявність уже готової ідентичності в мережі блокчейн дозволить уникнути необхідність постійної перевірки даних користу.

У даній концепції можна виділити три елементи: провайдер ідентичності, власник ідентичності та валідатор. Провайдером ідентичності може стати портал "ДіЯ", оскільки він містить персональні дані та може накладати цифровий підпис, власником ідентичності є сама особа, а валідатором буде виступати будь-яка організація чи особа, яка отримує дані ідентичності від власника та може перевірити їхню валідність перевіривши отримані дані у мережі блокчейн.

Висновки. Отже, дана концепція надає можливість створити цифрову ідентичність, яку можна пов'язати із конкретною особою, що дозволяє застосовувати її для автентифікації особи у різних державних сервісах, одночасно надаючи можливість керувати дозволами саме особі-власнику даних, що може підвищити довіру громадян до такої системи.

Інформаційні джерела

1. He X., Yang X. Authentication and authorization of end user in microservice architecture. Journal of physics: conference series. 2017. Т. 910. – С. 012060. URL: https://doi.org/10.1088/1742-6596/910/1/012060.

2. Про внесення змін до Положення про Систему BankID Національного банку України : Постанова Нац. банку України від 01.09.2023 № 105. URL: https:// zakon.rada.gov.ua/ laws/show/v0105500-23#Text.

3. BankID. BankID. URL: https://bankid.org.ua/.

4. У "Резерв+" після тестування відстрочок стався технічний збій: проблеми із входом. hromadske. URL: https://hromadske.ua/suspilstvo/233932-u-rezerv-pislia-testuvannia-vidstrochok-stavsia-tekhnichnyy-zbiy-problemy-iz-vkhodom (дата звернення: 19.11.2024).

5. Soltani R., Nguyen U. T., An A. A survey of self-sovereign identity ecosystem. Security and communication networks. 2021. Т. 2021. – С. 1–26. URL: https://doi.org/ 10.1155/ 2021/8873429.

6. Побережник В., Опірський І. Розробка концепції методу використання технології блокчейн для побудови системи обміну повідомленнями. Ukrainian information security research journal. 2023. Т. 25, № 2. – С. 62–70. URL: https://doi.org/ 10.18372/2410-7840.25.17673.

7. Poberezhnyk V., Opirskyy I. Developing of blockchain method in message interchange systems // CEUR Workshop Proceedings. – 2023. – Vol. 3421 : Proceedings of the Cybersecurity providing in information and telecommunication systems co-located with International conference on problems of infocommunications. Science and technology (PICST 2023) Kyiv, Ukraine, February 28, 2023 (online), pp. 148–157.

8. Upgradeable smart contracts: explanation & security concerns – hacken. Hacken. URL: https://hacken.io/discover/upgradeable-smart-contracts/.

9. Balatska Valeriia, Poberezhnyk Vasyl, Opirskyy Ivan. Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR // CEUR Workshop Proceedings. – 2024. – Vol. 3800 : Cyber security and data protection 2024. Proceedings of the cyber security and data protection workshop (CSDP 2024), Lviv, Ukraine, June 30, 2024 (online), pp. 70–80.

10. Дія. Підпис. "ДІЯ" | Кваліфікований електронний підпис. URL: https://ca.diia.gov.ua/faq_diia_id.

УДК 355.45:004.056.5

КРИТИЧНА ІНФРАСТРУКТУРА ПІД ЧАС ВІЙНИ: ЗАХИСТ ВІД КІБЕРАТАК ТА ВІДНОВЛЕННЯ СИСТЕМ

Костянтин РОТАНЬ
Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *This paper examines the importance of protecting critical infrastructure from cyberattacks during wartime, as well as strategies for recovering from attacks. It outlines the main threats, protection methods, including encryption, monitoring, physical security, and the importance of recovery planning to ensure the stability and security of the country.*
Keywords: *critical infrastructure, cyber threats, cloud technologies, system recovery, cybersecurity, encryption, blockchain, staff training, backups.*

Анотація. *В цій роботі розглядається важливість захисту критичної інфраструктури від кібератак під час війни, а також стратегії її відновлення після атак. Окреслюються основні загрози, методи захисту, включаючи шифрування, моніторинг, фізичну безпеку, а також важливість планування відновлення для забезпечення стабільності та безпеки країни.*
Ключові слова: *критична інфраструктура, кіберзагрози, хмарні технології, відновлення систем, кібербезпека, шифрування, блокчейн, навчання персоналу, резервні копії.*

Критична інфраструктура – це об'єкти, які є надзвичайно важливими для функціонування суспільства та економіки країни. До такої інфраструктури відносяться в першу чергу об'єкти оборони, а також ті, що забезпечують життєво важливі послуги та комунікацію. Це можуть бути електростанції, системи водопостачання, місця зберігання та виготовлення харчових продуктів, важливі транспортні вузли, телекомунікаційні мережі, медичні установи та багато інших пріоритетних об'єктів. Безпека цих об'єктів та їх функціонування як у нормальних умовах, так і в умовах надзвичайних ситуацій, таких як воєнний стан – один із пріоритетів держави [1].

У сучасних умовах кіберзагрози стають не менш важливими, ніж традиційні воєнні атаки. Зростання технологічної залежності держав від комп'ютерних мереж і програмного забезпечення призводить до того, що саме через них можуть бути здійснені нападні дії, здатні спричинити хаос у критичних сферах. Кібернапади на інфраструктуру можуть бути різного характеру – від атаки на сервери та мережі, які призводять до відмови в обслуговуванні (DDoS-атаки), до проникнення в контрольні системи (*наприклад*, SCADA), що забезпечують управління енергетичними, водними або транспортними мережами. Такі атаки можуть знищити або зашифрувати важливі дані, заблокувати доступ до життєво важливих систем і навіть викликати техногенні катастрофи.

Ще на початку повномасштабного вторгнення Національний банк України дозволив гравцям фінансового ринку розміщувати свою інфраструктуру та сервіси у хмарних сервісах і дата-центрах на території Європейського Союзу.

Це рішення стало одним із ключових у забезпеченні безперервної діяльності фінансового сектору, адже стало можливим використовувати європейські дата-центри та публічні хмарні сервіси: Amazon, Google Cloud, Azure та інші. У перші тижні й місяці війни український бізнес робив проєкти міграції, які раніше планувалися і впроваджувалися роками.

Цей підхід дав змогу компаніям мінімізувати ризики, пов'язані з фізичною безпекою IT-інфраструктури та забезпечити доступність і надійність послуг для своїх клієнтів.

До того ж у перший рік повномасштабного вторгнення більшість хмарних провайдерів надавали безоплатну можливість українським бізнесам користуватися хмарними послугами. Знаю, що дуже багато фінансових компаній скористалися такою можливістю.

Захист критичної інфраструктури від кіберзагроз вимагає комплексного підходу, що поєднує технічні, організаційні та правові заходи. Серед основних аспектів такого захисту – постійний моніторинг мереж і виявлення аномалій, що дозволяє вчасно реагувати на потенційні загрози. Одним із ключових елементів є створення та впровадження технологій шифрування, які дозволяють захистити дані від несанкціонованого доступу. Крім того, необхідно забезпечити фізичну безпеку критичних об'єктів, таких як центри обробки даних, сервери та інші важливі елементи інфраструктури, щоб убезпечити їх від нападів або саботажу.

Особливу увагу необхідно приділяти навчанню персоналу, адже багато кіберзагроз виникають через людський фактор – помилки або необережність працівників. Регулярні тренінги та підвищення обізнаності допомагають мінімізувати ці ризики. Водночас інтеграція новітніх технологій, таких як блокчейн, може додатково забезпечити прозорість і захищеність важливих транзакцій та даних.

Проте навіть найсучасніші системи захисту не можуть гарантувати повну недоступність до кіберзагроз. Тому важливим аспектом є здатність держави до швидкого відновлення після кібератаки. У випадку зламу або іншої серйозної кіберінцидентної ситуації критична інфраструктура повинна мати чітко визначений план відновлення, який включає в себе механізми відновлення резервних копій даних, перенаправлення трафіку на резервні сервери і повернення доступу до життєво важливих послуг. Ключовим є також наявність резервних копій даних, які дозволяють швидко відновити втрачену інформацію.

До того ж, хмарні технології, що забезпечують надійне зберігання і доступ до даних через глобальні мережі, значно спрощують процес відновлення

після атаки, дозволяючи забезпечити функціонування навіть за умов локальних уражень. Важливо також після кожної кіберінциденту проводити детальний аналіз, щоб з'ясувати, як атака стала можливою, та вдосконалити системи захисту з урахуванням нових загроз.

Важливі кроки для підвищення кібербезпеки:

– *Правильне використання паролів*. Використовувати складні паролі, що складаються з різних символів, цифр і літер, регулярно їх змінювати та не використовувати однакові паролі для різних сервісів.

– *Захист від фішингових атак*. Не відкривати підозрілі листи та не переходити за сумнівними посиланнями. Перевіряти справжність відправника перед відкриттям вкладених файлів. Використовувати антифішингові програми для захисту від шкідливих посилань та електронних листів.

– *Захист особистих даних*. Не ділитися особистими даними через незахищені канали зв'язку. Використовувати двофакторну автентифікацію для доступу до важливих акаунтів. Шифрувати важливі файли та інформацію.

– *Регулярне оновлення програмного забезпечення*. Оновлювати операційні системи та програмне забезпечення до останніх версій. Використовувати антивірусні програми й регулярно перевіряти пристрої на наявність шкідливих програм.

– *Навчання та підвищення обізнаності*. Регулярно проходити навчання з кібербезпеки та бути в курсі нових загроз [3].

Висновки. Таким чином, захист критичної інфраструктури від кіберзагроз і здатність до її відновлення після атак є основою безпеки та стабільності країни в умовах війни. Сучасні технології та ефективне управління цими загрозами можуть значно знизити ризики і мінімізувати наслідки для громадян і економіки, забезпечивши нормальне функціонування держави навіть у найскладніших умовах.

Інформаційні джерела

1. Все, що ви повинні знати про об'єкти критичної інфраструктури в Україні. Головні новини з України сьогодні – Kyiv Post. URL: https://www.kyivpost.com/uk/post/28283 (дата звернення: 18.11.2024).

2. Проєкт USAID "Кібербезпека критично важливої інфраструктури України" провів перший "Діалог про кібербезпеку" – Aspen Institute Kyiv. Aspen Institute Kyiv. URL: https://aspeninstitutekyiv.org/proiekt-usaid-kiberbezpeka-krytychno-vazhlyvoi-infrastruktury-ukrainy-proviv-pershyi-dialoh-pro-kiberbezpeku/ (дата звернення: 18.11.2024).

3. Лісничий Г. Кіберзахист під час війни: виклики та рішення – ProIT. ProIT: медіа для профі в IT. URL: https://proit.ua/kibierzakhist-pid-chas-viini-vikliki-ta-rishiennia/ (дата звернення: 18.11.2024).

УДК 004.056

ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБМІНУ ПОВІДОМЛЕННЯМИ

Тетяна КОРОБЕЙНІКОВА
Богдан ОДІНЦОВ
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *The study substantiates the choice of messaging system implementation tools, including FastAPI, PostgreSQL, JWT, WebSocket, OAuth2, and Flutter. Modern approaches to ensuring data integrity are reviewed, such as encryption, hashing, digital signatures, and security protocols, which provide reliability, scalability, security, platform adaptability, integration simplicity, efficiency, and compliance with the requirements of the modern digital environment.*

Keywords: *information system, messaging, data integrity.*

Анотація. *У роботі обґрунтовано вибір засобів для реалізації системи обміну повідомленнями, зокрема FastAPI, PostgreSQL, JWT, WebSocket, OAuth2 та Flutter. Оглянуто сучасні підходи до забезпечення цілісності даних: шифрування, хешування, електронні підписи й протоколи безпеки, що забезпечують надійність, масштабованість, захищеність, адаптивність платформи, простоту інтеграції, ефективність та відповідність вимогам сучасного цифрового середовища.*

Ключові слова: *інформаційна система, обмін повідомленнями, цілісність даних.*

Забезпечення цілісності даних у публічних мережах є критично важливим завданням у сучасному цифровому світі, де обмін інформацією відбувається постійно і часто через ненадійні середовища. Шифрування, хешування, електронні підписи, а також різноманітні протоколи безпеки, забезпечують необхідний рівень захисту даних та дозволяють мінімізувати ризики їх підробки або втрати [1–2].

Метою дослідження є розробка архітектури інформаційної системи обміну повідомленнями із забезпеченням високого рівня цілісності, конфіденційності та надійності.

Для досягнення поставленої мети сформуємо такі *задачі*:

– аналіз існуючих підходів до забезпечення цілісності даних у публічних мережах;

– розробка архітектури інформаційної системи обміну повідомленнями;

– реалізація та тестування прототипу системи;

– оцінка ефективності запропонованого рішення.

Методи проведення дослідження: аналіз наукових публікацій, стандартів безпеки та сучасних практик розробки інформаційних систем; практичне впровадження розробленої архітектури з використанням обраних технологій.

Наукова новизна: запропоновано комплексну архітектуру системи обміну повідомленнями, яка поєднує сучасні технології та криптографічні методи для забезпечення цілісності даних.

Практична цінність. Результати дослідження можуть бути використані для створення захищених корпоративних систем обміну повідомленнями, банківських сервісів, додатків для електронного документообігу та інших критичних застосунків

Задача забезпечення цілісності інформації в публічній мережі під час реалізації інформаційної системи обміну повідомленнями. Один із ключових підходів до забезпечення цілісності даних – це шифрування. Механізми шифрування гарантують, що навіть у випадку перехоплення або втрати доступу до даних треті сторони не можуть прочитати інформацію без спеціальних ключів. Сучасні криптографічні алгоритми AES та RSA забезпечують високий рівень безпеки під час передавання даних через публічні мережі.

Хешування даних є іншим потужним інструментом, що дозволяє перевіряти, чи не були змінені дані під час їх передавання. Хешування дозволяє створити унікальний відбиток для кожного повідомлення або файлу. SHA-256 забезпечує надійний механізм перевірки цілісності даних.

Електронні підписи також відіграють важливу роль у забезпеченні цілісності даних і дають можливість перевірити авторство повідомлення та переконатися, що його зміст не було змінено. Це дозволяє будувати довіру між сторонами, що обмінюються інформацією в публічних мережах. Електронні підписи використовуються у багатьох системах обміну повідомленнями, банківських транзакціях та інших критично важливих галузях.

Використання криптографічних протоколів SSL/TLS захищає передавання даних між клієнтами та серверами. Ці протоколи забезпечують шифрування даних під час їх передавання і аутентифікацію сторін, що обмінюються повідомленнями. SSL/TLS допомагають запобігти MITM-атакам та іншим видам несанкціонованого доступу.

Важливим є постійне оновлення та вдосконалення методів захисту даних у публічних мережах, оскільки загрози, пов’язані з кібератаками та вразливостями, еволюціонують.

Розробка архітектури інформаційної системи обміну повідомленнями. Ефективне забезпечення цілісності інформації у публічних мережах залежить від комплексного використання сучасних інструментів та технологій захисту даних. Поєднання шифрування, хешування, електронних підписів та криптографічних протоколів створює надійний фундамент для безпечної передавання інформації.

Поєднання сучасних засобів забезпечення цілісності інформації в системах обміну повідомленнями є необхідним для створення безпечних платформ. Проблеми, пов’язані з передавання даних у відкритих мережах, можуть бути успішно вирішені шляхом інтеграції таких інструментів, як

FastAPI для високопродуктивного веб-додатку, PostgreSQL для надійного збереження даних, JWT для захищеної аутентифікації та авторизації, а також WebSocket для обміну повідомленнями з використанням JWT в реальному часі. Розробка додатку із використанням цих технологій дозволяє побудувати платформу з високим рівнем безпеки та надійності. Такий підхід дозволить забезпечити цілісність, конфіденційність та безперервність передавання даних в умовах зростаючих кіберзагроз [3].

До процесу розробки архітектури потрібно підходити з увагою до деталей та з глобальним задумом, аби вона була масштабована, продумана та надавала можливість виконання ключових потреб додатку, була надійною та захищена від загроз. Головними критеріями архітектури системи є масштабованість, швидкість роботи, безпека даних, та простота в розробці та подальшій підтримці.

Обґрунтування вибору засобів реалізації інформаційної системи обміну повідомленнями. Для реалізації архітектури системи варто провести аналіз та вибір засобів для розробки. На основі цих критеріїв автор вибрав такі засоби реалізації.

1. Переваги використання FastAPI як бекенд-фреймворку. Висока продуктивність: FastAPI є одним із найшвидших фреймворків для Python завдяки використанню асинхронної обробки запитів та базується на Starlette і Pydantic, що забезпечує швидке виконання запитів, особливо при великих навантаженнях. Асинхронність: можливість обробляти асинхронні запити забезпечує високу ефективність при роботі з WebSocket, обробкою багатьох запитів одночасно і запитами до бази даних. Проста інтеграція з OpenAPI: FastAPI автоматично створює документацію API у форматі OpenAPI, що полегшує тестування та подальшу підтримку. Безпечність: вбудована підтримка OAuth2, JWT та інших засобів аутентифікації та авторизації. Зручність використання: завдяки анотаціям типів Python і Pydantic, розробка API є інтуїтивно зрозумілою, що скорочує час на розробку та знижує ризик помилок.

2. PostgreSQL є оптимальним вибором для системи, яка працює з чутливими даними користувачів [4]. Реляційна структура даних: PostgreSQL – реляційна СУБД, яка ідеально підходить для застосунків з високою вимогою до надійності та структурованості даних. Підтримка складних запитів: PostgreSQL дозволяє ефективно працювати з SQL-запитами та підтримує складні операції з даними. Безпека: Механізми управління доступом та шифрування даних забезпечують високий рівень безпеки. Масштабованість: PostgreSQL підтримує великі обсяги даних, можливість горизонтального масштабування та паралельну обробку запитів, що дозволяє системі рости разом із зростанням кількості користувачів. Розширюваність: PostgreSQL підтримує безліч розширень (PostGIS для геолокаційних даних), що розширює функціональність без необхідності змінювати базову архітектуру.

3. Переваги використання JWT (JSON Web Tokens) для аутентифікації та авторизації. Безпечність передавання даних: JWT дозволяє передавати зашифровані токени між клієнтом та сервером, що захищає дані користувача. Самодостатні токени: JWT містить у собі всю інформацію, необхідну для авторизації, що дозволяє уникнути додаткових запитів до сервера для перевірки сесій. Простота використання: JWT легко інтегрувати з протоколом OAuth2, що робить його ідеальним вибором для забезпечення доступу до ресурсів. Швидкість: на відміну від сесійного зберігання, JWT не потребує постійного зберігання на сервері, що зменшує затримку при перевірці автентичності.

4. Використання WebSocket для роботи в режимі реального часу. Двосторонній зв'язок: WebSocket забезпечує постійне з'єднання між клієнтом і сервером, що дозволяє системі обмінюватися даними у реальному часі. Ефективність: WebSocket оптимізований для обміну повідомленнями у реальному часі, що знижує затримку порівняно з традиційними HTTP-запитами. Ідеально підходить для інтерактивних застосунків: чати, онлайн-моніторинг.

5. OAuth2 як механізм безпеки для керування доступом. Міжсистемна сумісність: OAuth2 є стандартним протоколом для авторизації, що дозволяє інтегрувати систему з іншими сервісами, такими як Google або Facebook, для авторизації користувачів. Можливість гранульованого контролю доступу: OAuth2 дозволяє налаштовувати рівень доступу для кожного користувача, та до окремих ресурсів. Захист ресурсів: OAuth2 надає можливість безпечного доступу до ресурсів, мінімізуючи ризик несанкціонованого доступу та витоків.

6. Flutter. Причини використання Flutter для розробки клієнтської частини. Кросплатформеність: Flutter дозволяє створювати додатки для Android та iOS з одним базовим кодом, що суттєво знижує витрати на розробку. Висока продуктивність: Dart (мова програмування, яка використовується у Flutter) компілюється у рідний код, що забезпечує високу швидкість роботи додатка. Гарний та зручний інтерфейс: Flutter дозволяє створювати адаптивні, привабливі та сучасні інтерфейси завдяки вбудованим компонентам і бібліотекам. Гнучкість: розробка в Flutter надає можливості швидкого тестування та редагування інтерфейсу без компіляції коду кожного разу (завдяки функції Hot Reload). Розвинена екосистема: бібліотеки та плагіни Flutter полегшують інтеграцію із зовнішніми сервісами, зокрема підтримку аутентифікації, обробки HTTP-запитів та роботи з WebSocket.

Висновки. Ефективне забезпечення цілісності інформації у публічних мережах потребує комплексного підходу та використання сучасних технологій. Інтеграція шифрування, хешування, електронних підписів, криптографічних протоколів та новітніх засобів розробки (FastAPI, PostgreSQL, JWT, WebSocket, OAuth2, Flutter) створює надійну платформу для захисту даних. Цей підхід дозволяє забезпечити безперервність, конфіденційність і цілісність передавання інформації навіть за умов зростаючих кіберзагроз.

Інформаційні джерела

1. Ковалевський В., Вакалюк Т. Огляд сучасних систем захисту електронних сервісів. Herald of khmelnytskyi national university. Technical sciences, 2024, 337.3 (2). – С. 176–182.

2. Борисенко О., Тимошенко А. Огляд методів захисту персональних даних у хмарному середовищі. Інфокомунікаційні та комп'ютерні технології, 2024, 1.07. – С. 31–34.

3. Коробейнікова Т.І., Савицька Л. А. Удосконалений метод розробки API підвищеної швидкодії. Інформаційні технології та комп'ютерна інженерія. – Вінниця, 2021. – №1 (том 50), С. 31–35.

4. Korobeinikova T., Chekhmestruk R., Mykhaylov P., Romanyuk O., Romanyuk O. and Achanyar H., "The Fault-Resistant Web Application Infrastructure Using Autoscaling", 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland, 2023, pp. 479–482.

УДК 004.056.5

МОДЕЛЬ КЛАСИФІКАЦІЇ ІНФОРМАЦІЇ ЗГІДНО З ВИМОГАМИ SOC 2 TYPE 2

Олег ДЕЙНЕКА
Олег ГАРАСИМЧУК
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *SOC2 Type 2 is an important certification that validates an organization's ability to provide services in accordance with trust relationship criteria that cover security, availability, processing integrity, confidentiality and privacy. Data classification is a critical first step in creating a robust data security strategy, after which an organization knows what data it owns and determines the level of sensitivity of that data, which determines what security measures should be in place.*

Keywords: *SOC2 Type 2, storage standards, data classification, data storage, data security.*

Анотація*. У цій роботі розглянута розробка політики класифікації даних для відповідності SOC2 Type 2. SOC2 Type 2 є важливою сертифікацією, яка підтверджує здатність організації надавати послуги відповідно до критеріїв довірливих відносин, що охоплюють безпеку, доступність, цілісність обробки, конфіденційність та приватність. Класифікація даних є критичним першим кроком у створенні надійної стратегії безпеки даних, оскільки вона допомагає організаціям зрозуміти, які дані вони мають, і призначає рівень чутливості цим даним, що визначає, які заходи безпеки повинні бути застосовані.*

Ключові слова: *SOC2 Type 2, стандарти зберігання, класифікація даних, зберігання даних, безпека даних.*

Вступ. У сучасному світі відбувається стрімке зростання обсягів інформаційних активів, які включають значну частку критично важливої інфор-

мації. Ці дані вимагають ретельної класифікації за різними характеристиками та параметрами, забезпечення їх надійного зберігання, безпечної передачі, а також ефективного захисту від несанкціонованого доступу. Водночас останніми роками спостерігається постійне збільшення кількості потенційних атак на інформаційні ресурси [1–2]. Стандарти безпеки дозволяють краще зрозуміти, як саме установа контролює доступ до даних і забезпечує їх безпеку та конфіденційність [3–4].

Основні частина. SOC2 Type 2 [5] вимагає від організацій ефективного управління конфіденційністю, приватністю та безпекою інформації відповідно до Критеріїв Довірчих Послуг. Політика класифікації даних є критичним компонентом для відповідності цим критеріям, особливо критерію безпеки. Вона повинна включати ідентифікацію типів даних, встановлення рівнів класифікації, визначення ролей і відповідальності, вимоги до обробки та контроль доступу. Політика також повинна передбачати регулярне навчання співробітників, аудит та моніторинг, а також інтеграцію з планом реагування на інциденти. Важливо залучати досвідчених експертів з відповідності або аудиторів для розробки та підтримки політики класифікації даних, щоб забезпечити відповідність стандартам SOC2 Type 2.

Розглядаючи розробку моделі ми виділяємо наступні ролі для управлінню моделлю:

– *Працівник*: Працівник відповідає за дотримання політики класифікації даних, правильне оброблення даних згідно з їх класифікацією та повідомлення про будь-які інциденти або порушення.

– *Куратор даних*: Куратор даних відповідає за управління та контроль даних в організації, забезпечуючи правильну класифікацію даних, дотримання політики класифікації та використання даних у відповідності до законодавчих та регуляторних вимог.

– *Аудитор*: Аудитор відіграє ключову роль у оцінці відповідності організації вимогам SOC2, включаючи політику класифікації даних, шляхом незалежного перегляду політик, процесів та контролю.

– *Адміністратор*: Адміністратор відповідає за підтримку безперебійної роботи IT-систем організації, включаючи розгортання нових версій додатків, моніторинг продуктивності систем та встановлення останніх оновлень безпеки для всього оперативного персоналу.

– *Система єдиного входу (SSO)*: Система SSO відповідає за управління автентифікацією користувачів та контролем доступу, забезпечуючи, що користувачі мають доступ лише до тих даних, до яких вони авторизовані відповідно до своїх ролей та класифікації даних.

– *Система обробки*: Система обробки забезпечує безпечну обробку, зберігання та передачу даних відповідно до політики класифікації даних, а також оптимізує процес пошуку даних за допомогою індексації даних і методів машинного навчання.

– *Управління IT-послугами (ITSM)*: ITSM відповідає за надання IT-послуг, що підтримують політику класифікації даних, включаючи управління доступом, виконання запитів та управління інцидентами.

Основні дії та процеси для обробки та класифікації даних:

Пропонуємо таку структуру збору, обробки та класифікації даних відповідно до стандарту SOC2 Type 2 (рис. 1).

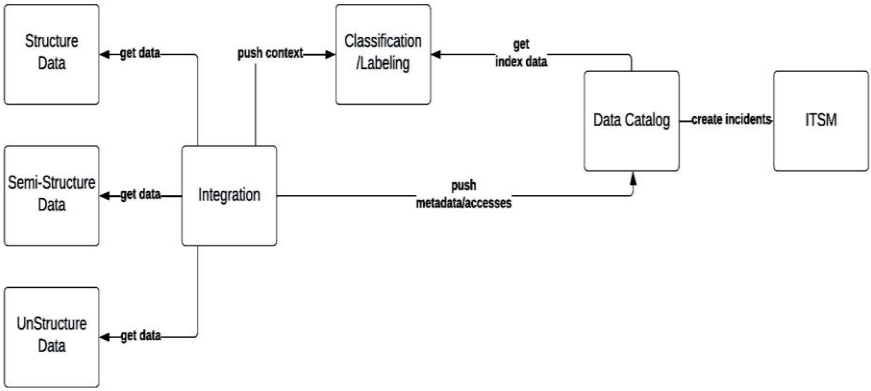


Рисунок 1 – Потік даних при обробці та класифікації інформації

Коли з'являється нова інформація про клієнта або категорія, її слід додати до Каталогу даних клієнтів. Додавання нової інформації про клієнта може включати збір додаткових деталей з будь-якою відповідною інформацією. Створення нової категорії може передбачати створення нової групи або сегментацію існуючих даних клієнтів на різні категорії. Це робиться для підвищення ефективності Каталогу даних клієнтів та прийняття більш обґрунтованих бізнес-рішень. Важливо забезпечити, щоб нова інформація або категорія збиралися та зберігалися відповідно до регламентів захисту даних та законів про конфіденційність клієнтів.

Зміна рівня чутливості даних означає, що рівень важливості або конфіденційності даних збільшився або зменшився. Якщо раніше неконфіденційні дані стали конфіденційними через зміни в регулюваннях, бізнес-практиках або юридичних вимогах, рівень чутливості даних збільшився. Навпаки, якщо конфіденційні дані стали менш важливими або цінними через зміни в бізнес-практиках або юридичних вимогах, рівень чутливості даних зменшився. Важливо регулярно переглядати та оцінювати рівень чутливості даних, щоб забезпечити їх адекватний захист та внести необхідні корективи в заходи безпеки та контроль доступу.

Якщо дані, що збираються для конкретної категорії, змінюються або розширюються, опис цієї категорії може потребувати редагування для відо-

браження нових даних. Редагування опису існуючої категорії даних клієнтів зазвичай робиться для уточнення та відображення змін у зібраних даних.

Опис методу оброки класифікації у діаграмі потоку даних

Крок 1: Розуміння типів даних, що належать вашій компанії

Перший крок у створенні діаграми потоку даних полягає в розумінні типів даних, які належать вашій компанії, включаючи структуровані, напівструктуровані та неструктуровані дані.

Крок 2: Розуміння метаданих, пов'язаних з вашими даними

Після ідентифікації типів даних наступним кроком є розуміння метаданих, які надають інформацію про інші дані, такі як автор, дата створення та розмір файлу.

Крок 3: Використання інструментів інтеграції для управління та зберігання даних

Необхідно використовувати інструменти інтеграції для вилучення, трансформації та завантаження даних у сховище, що дозволяє консолідувати дані в одному місці для легшого управління та аналізу.

Крок 4: Створення моделі даних

Створення моделі даних, яка є візуальним представленням взаємозв'язків між різними елементами даних, що допомагає організувати та структурувати дані.

Крок 5: Класифікація та зв'язування даних з метаданими

Необхідно класиифікувати дані та зв'язати їх з відповідними метаданими, призначаючи рівень чутливості даним на основі їх важливості та потенційного впливу у разі втрати або викрадення.

Крок 6: Візуалізація та управління даними

Створіть додаток для візуалізації та управління даними, який забезпечує зручний інтерфейс для доступу, аналізу та маніпулювання даними, а також включає логіку для управління доступом, запитами та інцидентами.

Висновки. Розробка політики класифікації даних для відповідності SOC2 Type 2 є складним, але важливим завданням для організацій. SOC2 Type 2 є значною сертифікацією, яка підтверджує здатність організації відповідати Критеріям Довірчих Послуг, що включають безпеку, доступність, цілісність обробки, конфіденційність та приватність. Основні цілі класифікації даних полягають в організації та управлінні даними таким чином, щоб підвищити їх захист і узгодити з загальною стратегією безпеки даних організації. Для ефективного захисту чутливої інформації та підтримки цілісності надання послуг організаціям необхідно подолати численні виклики та врахувати різні аспекти, такі як розуміння обсягу даних, узгодження з Критеріями Довірчих Послуг, балансування безпеки та зручності, навчання та підвищення обізнаності, регулярні оновлення та огляди, визначення рівнів класифікації, забезпечення послідовності, автоматизація класифікації, інтеграція з іншими політиками та контролями, робота з третіми сторонами, моніторинг та виконання, а також дотримання юридичних та регуляторних вимог.

Інформаційні джерела

1. Matturdi B., Zhou X., Li S. and Lin F., "Big Data security and privacy: A review", in China Communications, vol. 11, no. 14, pp. 135–145, 2014. doi: 10.1109/CC. 2014. 7085614.
2. Islam M. N., Zaki T., Uddin M. S., Hasan M. M. Security threats for big data: An empirical study. Int J Inf Commun Technol Human Dev (IJICTHD). 2018, 10(4), pp. 1–18. doi: 10.4018/IJICTHD.2018100101.
3. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirement. URL: https://www.iso.org/ standard/ 27001, 10.11.2024.
4. URL: https://www.isaca.org/resources/isaca-journal /issues/2016/volume-6/is-audit-basics-the-domains-of-data-and-information-audits, Ulf Mattsson, Ed Gelbstein, Ph.D, 2016.
5. SOC 2 Compliance Documentation. URL: https://secureframe.com/hub/soc-2/ compliance-documentation/, 10.11.2024.

УДК 004.056:005.8

ВПЛИВ СУЧАСНИХ ЗАГРОЗ НА КІБЕРБЕЗПЕКУ ТА ЕФЕКТИВНІСТЬ ПІДХОДІВ ДО ЇХ ЗАПОБІГАННЯ

Олександр САФРОНОВ
Василь ЛУЧИК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The paper explores new approaches to cybersecurity in the face of the increasing complexity of modern threats, such as malware, phishing, DDoS attacks, and advanced persistent threats (APTs). It examines innovative strategies, including zero-trust architecture, network segmentation, and the use of artificial intelligence and cloud technologies to detect and neutralize threats. It emphasizes the importance of the human factor, the need for user training, and increasing awareness of cyber hygiene. It emphasizes the importance of integrating modern technologies into cyber defense strategies to effectively respond to dynamically changing challenges.*

Keywords: *cybersecurity, modern threats, zero-trust architecture, artificial intelligence, cloud technologies, cyber hygiene, network segmentation, machine learning.*

Анотація. *У роботі досліджуються нові підходи до забезпечення кібербезпеки в умовах зростання складності сучасних загроз, таких як зловмисне програмне забезпечення, фішинг, DDoS-атаки та вдосконалені постійні загрози (APT). Розглянуто інноваційні стратегії, зокрема архітектуру нульової довіри, сегментацію мережі, використання штучного інтелекту та хмарних технологій для виявлення й нейтралізації загроз. Акцентовано увагу на важливості людського фактора, необхідності навчання користувачів та підвищення обізнаності про кібергігієну. Підкреслено значення інтеграції сучасних технологій у стратегії кіберзахисту для ефективного реагування на динамічно змінювані виклики.*

Ключові слова*: кібербезпека, сучасні загрози, архітектура нульової довіри, штучний інтелект, хмарні технології, кібергігієна, сегментація мережі, машинне навчання.*

У сучасному цифровому світі кібербезпека стає однією з найважливіших сфер захисту інформаційних активів, а зростання складності кіберзагроз ставить перед професіоналами нові виклики. Зловмисне програмне забезпечення, фішинг, DDoS-атаки, соціальна інженерія та вдосконалені постійні загрози (APT) змушують компанії застосовувати нові підходи до захисту своїх систем. Зі збільшенням кількості пристроїв, підключених до Інтернету, і використанням хмарних технологій ризик загроз значно зріс. Традиційні методи захисту, такі як антивірусні програми, брандмауери та системи виявлення вторгнень, поступово стають менш ефективними, оскільки кіберзлочинці використовують сучасні технології та методи для обходу заходів безпеки.

На цьому тлі з'являються нові підходи, такі як архітектура нульової довіри, сегментація мережі та штучний інтелект для аналізу загроз, щоб забезпечити більш ефективну відповідь на сучасні виклики.

Актуальність даної теми зумовлена постійною еволюцією загроз та негативним впливом, який вони мають на приватний бізнес, державні установи та суспільство в цілому. Забезпечення високого рівня кібербезпеки вимагає адаптації існуючих методів захисту та впровадження нових стратегій, які можуть реагувати на кіберзагрози, що швидко змінюються.

Крім теми впливу сучасних загроз на кібербезпеку, важливо звернути увагу на деякі важливі аспекти, які визначають ефективність підходу до протидії кібератакам. По-перше, загрози стають більш цілеспрямованими та персоналізованими, що вимагає нових методів виявлення та реагування. Традиційних методів, заснованих на сигнатурах і правилах, часто недостатньо, оскільки кіберзлочинці все частіше використовують атаки, які оминають традиційні системи захисту.

Крім технічних заходів, важливу роль відіграє і людський фактор. Зломи часто відбуваються через недостатню обізнаність користувачів про кіберзагрози або помилки, пов'язані з недотриманням кібергігієни. У цьому контексті програми навчання та підвищення обізнаності співробітників організації стали невід'ємною частиною сучасної кібербезпеки. Удосконалення технологій штучного інтелекту та машинного навчання зробили можливим аналізувати великі обсяги даних у режимі реального часу для виявлення аномалій у поведінці мережі та системи. Ці підходи дозволяють швидше реагувати на потенційні загрози та скорочують час реагування на інциденти.

Хмарні обчислення також відкривають нові можливості для кібербезпеки, зокрема завдяки використанню масштабованих рішень для захисту даних і виявлення загроз. Однак це також створює нові ризики, пов'язані з централізацією даних і залежністю від хмарних провайдерів. Одним із перспективних напрямків залишаються архітектури нульової довіри. Він жорстко контролює доступ до ресурсів і перевірку всіх запитів, незалежно від того, надходять вони з внутрішньої чи зовнішньої мережі.

Висновки. Цей підхід стає все більш важливим з огляду на збільшення кількості віддалених працівників і зростання популярності гібридної інфраструктури.

Інформаційні джерела

1. Для складання тези про вплив сучасних загроз на кібербезпеку та ефективність підходів до їх 1. Stallings W., & Brown L. (2018). Computer Security: Principles and Practice. Pearson. URL: Офіційна сторінка книги на Pearson (дата звернення: 18.11.2024).

2. FireEye (2021). M-Trends 2021: Insights into Today's Cyber Attacks and Trends. FireEye Report. URL: Деталі на сайті FireEye (дата звернення: 18.11.2024).

3. NIST (2020). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. URL: Завантажити з NIST (дата звернення: 18.11.2024).

4. ISO/IEC 27001 (2013). Information technology – Security techniques – Information security management systems – Requirements. URL: Опис стандарту на офіційному сайті ISO (дата звернення: 18.11.2024).

5. Kaspersky Lab (2021). Advanced Persistent Threat (APT) Trends Report, URL: Деталі на сайті Kaspersky (дата звернення: 18.11.2024).

УДК 343.9:159.9

ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРЗЛОЧИНИ: КРИМІНАЛЬНА ТА ЦИВІЛЬНА. СОЦІАЛЬНО-ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ

Максим РАК

Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article analyzes the provisions of Chapter XVI of the Criminal Code of Ukraine, which regulate liability for the main types of cybercrimes. The articles that cover unauthorized interference in the operation of systems, creation and distribution of malicious software, illegal circulation of information with limited access, violation of the rules for operating systems and mass disruptions to their work are considered. The key differences between the articles are identified, as well as the problems of their application in practice. The need to improve the legislative framework for effective combating modern cyber threats, including attacks using artificial intelligence and social engineering is emphasized.*

Keywords: *cybercrimes, Criminal Code of Ukraine, unauthorized interference, malicious software, DDos attacks, social engineering, cybersecurity, economic crimes, international standards.*

Анотація. *У статті проаналізовано положення Розділу XVI Кримінального кодексу України, що регулюють відповідальність за основні види кіберзлочинів. Роз-*

глянуто статті, які охоплюють несанкціоноване втручання у роботу систем, створення та поширення шкідливого програмного забезпечення, незаконний обіг інформації з обмеженим доступом, порушення правил експлуатації систем і масові перешкоди їх роботі. Визначено ключові відмінності між статтями, а також проблеми їх застосування на практиці. Підкреслено необхідність удосконалення законодавчої бази для ефективної боротьби з сучасними кіберзагрозами, включаючи атаки із застосуванням штучного інтелекту та соціальної інженерії.

Ключові слова: *кіберзлочини, Кримінальний кодекс України, несанкціоноване втручання, шкідливе програмне забезпечення, DDos-атаки, соціальна інженерія, кібербезпека, економічні злочини, міжнародні стандарти.*

Кіберзлочини в Україні регулюються Розділом XVI Кримінального кодексу, що встановлює кримінальну відповідальність за шість основних типів порушень. Серед них: несанкціоноване втручання у роботу систем (ст. 361), створення та розповсюдження шкідливого ПЗ (ст. 361-1), незаконний збут інформації з обмеженим доступом (ст. 361-2), порушення правил експлуатації систем (ст. 363) та перешкоджання їхній роботі через масові дії (ст. 363-1). Стаття 361: Несанкціоноване втручання у роботу систем**.** Стаття передбачає кримінальну відповідальність за дії, які призводять до втрати, блокування, або підробки інформації.

Покарання сягає шести років позбавлення волі за значну шкоду або повторні злочини. Це класичний приклад хакерства, що включає “зломи” систем із порушенням їхньої цілісності. У порівнянні з іншими статтями, 361 визначає дії, що безпосередньо впливають на безперервність роботи системи. Стаття 361-1: Шкідливе програмне забезпечення**.** Ця стаття охоплює створення, збут і розповсюдження шкідливих програм чи технічних засобів, спрямованих на завдання шкоди системам. Відповідальність передбачає до п’яти років позбавлення волі.

Основна відмінність від статті 361 полягає в тому, що 361-1 стосується підготовчих дій, які можуть передувати зламам, але не обов’язково супроводжуються втручанням. Стаття 361-2: Незаконний збут інформації з обмеженим доступом передбачає відповідальність за продаж конфіденційної або захищеної інформації, зокрема даних із державних реєстрів. Покарання може сягати п’яти років позбавлення волі. У порівнянні з 361-1, ця стаття регулює економічні злочини, що виникають із доступу до чутливих даних, без прямого втручання у роботу систем.

Стаття 363: Порушення правил експлуатації систем фокусується на недотриманні встановлених правил використання систем і мереж, що спричинило значну шкоду. Вона відрізняється від 361 тим, що передбачає відповідальність за порушення з боку осіб, які мають право доступу до систем, але

діють недбало або безвідповідально. Через складність фіксації таких злочинів ця стаття рідко застосовується. Стаття 363-1: Масові перешкоди роботі систем передбачає відповідальність за дії, що порушують роботу систем через масове розсилання повідомлень, як-от DDos-атаки. Вона передбачає до п'яти років позбавлення волі за значну шкоду. Ця стаття має найбільшу схожість зі ст. 361, але ключова відмінність полягає у методі скоєння злочину – використанні масових дій, що паралізують систему.

Статті 361 і 361-1 акцентують на активних хакерських діях, тоді як 363 стосується професійної недбалості осіб із доступом до систем. Стаття 363-1 є продовженням 361, але акцентує на технологічно специфічних атаках, таких як спам чи DDos. 361-2, своєю чергою, виходить за межі атак, охоплюючи економічну діяльність із незаконного обігу даних.

На практиці розмежування між статтями викликає труднощі. *Наприклад*, дії, що одночасно включають розповсюдження шкідливого ПЗ (361-1) і втручання у роботу систем (361), часто кваліфікуються разом. Це потребує висококваліфікованої експертизи для правильного визначення складу злочину.

Україна, гармонізуючи своє законодавство з Конвенцією про кіберзлочинність, запровадила статті, що відповідають міжнародним стандартам. Це допомагає забезпечити співпрацю з іншими країнами в питаннях екстрадиції та розслідувань кіберзлочинів, особливо у випадках міжнародного характеру, як-от DDos-атаки чи транснаціональний збут даних.

Висновки. Статті Розділу XVI КК України утворюють комплексний підхід до боротьби з кіберзлочинами, від атак і створення шкідливого ПЗ до порушень експлуатації та торгівлі даними. Однак, для ефективного правозастосування необхідна більша деталізація окремих положень і їх гармонізація з сучасними кіберзагрозами, зокрема атаками із використанням штучного інтелекту та соціальної інженерії.

Інформаційні джерела

1. Правове регулювання відповідальності за кіберзлочини в Україні. URL: https://legalitgroup.com/pravove-regulyuvannya-vidpovidalnosti-za-kiberzlochini-v-ukrayini/ (дата звернення: 17.11.2024).

2. Кіберзлочинність, правове регулювання. URL: https://interfax.com.ua/news/press-release/756785.html (дата звернення: 16.11.2024).

3. Правові засади забезпечення кібербезпеки України в умовах цифрового комунікативного середовища. URL: https://chasprava.com.ua/index.php/journal/article/download/858/797/ (дата звернення: 17.11.2024).

4. Державне регулювання протидії кіберзлочинності в Україні. URL: https://pag-journal.iei.od.ua/archives/2024/40-2024/43.pdf (дата звернення: 17.11.2024).

УДК 621.372

ІДЕНТИФІКАЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ДІЯЛЬНОСТІ КОГНІТИВНОЇ СИСТЕМИ ОСОБИ В УМОВАХ ДІЇ АКТИВНИХ ЗАГРОЗ

***Богдан ДУРНЯК*[1]**
***Ростислав ТКАЧУК*[1,2]**
***Любомир СІКОРА*[1]**

[1]Національний університет "Львівська політехніка", м. Львів, Україна.
[2]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.

Abstract. *An urgent problem is the analysis of the mechanisms of activity in the IACU of the person and teams of performers in extreme situations, and the forecast of possible failures in decision-making due to mental tension. The processes of solving tasks and problems are the basis of the subconscious and conscious components of intellectual activity, and therefore it is important to form the concept of identifying the mechanisms of mental (intellectual) activity of a person.*

Key words*: information, identification, processes of intellectual activity, effects of threats on the cognitive system.*

Анотація. *Актуальною проблемою є аналіз механізмів діяльності в ІАСУ особи та команд виконавців в умовах екстремальних ситуацій, і прогноз можливих збоїв при прийнятті рішень за рахунок психічної напруженості. Процеси розв'язання задач та проблем є основою підсвідомої й свідомої компонент інтелектуальної діяльності, а тому важливим є формування концепції ідентифікації механізмів розумової (інтелектуальної) діяльності особи.*

Ключові слова: *інформація, ідентифікація, процеси інтелектуальної діяльності, дії загроз на когнітивну систему.*

Концепція функціональної системи П. Анохіна. Функціональна система виступає як сукупність елементів та процесів в ній з відповідною організаційною структурою та стратегією поведінки, що призводить до цільового результату при розв'язанні певного класу задач та проблем [1, 3–4, 7].

Основні елемент і характерні властивості:

– незмінність структури системи в процесі функціонування;
– афферентний синтез, як узагальнення потоків інформації;
– цілеорієнтація;
– прийняття рішень для реалізації локальної мети в набор пріорітетів;
– модель програми дій для реалізації рішень;
– модель результатів дій (акцетор дій);
– зворотний зв'язок та контроль результатів локальних дій.

Аффертний синтез стратегій поведінки:

– виявлення домінуючої мотивації (цілеорієнтація особи, системи);

– ситуаційна аферентація в зоні взаємодії система ⇔ об'єкт і готовність до дій;

– пам'ять образів ситуацій, набутих даних і знань, як інформаційна основа дій;

– пускова аферентація до виконання команд і дій на основі ініційованої стратегії поведінки.

Прийняття рішень – визначає вибір варіанту майбутньої дії на основі інформаційної оцінки ситуації та цілеорієнтації. При цьому:

– знижується число степенів свободи в системі альтернатив;

– вноситься визначеність в тактику і стратегію можливих дій та їх напрям;

– на основі процесу цілеорієнтації та напрямку дій формується модель результатів дій (акцептор дії) і програма послідовності дій;

– в ході виконання дій виконується порівняння результатів з програмою і акцептором дій;

– за рахунок зворотного зв'язку виконується оцінка степені досягнення мети і корекція руху в напрямку цільового стану.

Концепція Миллера Г., Галантера Е. планів і структури поведінки у вигляді моделі "ТОТЕ" – (тест → дія → тест → вихід на ціль) ґрунтується на розходженні програмного і реального рухів (розбаланс траєкторій в напрямку мети) та їх корекції з використанням зворотного інформаційного зв'язку.

Концепція Хекхаузена Х. і Голвітцера П. теорії чотирьох стадій дій (модель Рубікона) характеризується такою схемою аналізу психологічного контролю дій:

– перший етап – стадія перед-рішення, яка полягає у виборі варіанту майбутньої дії з ціллю реалізації мети;

– другий етап – прийняття рішення – формування намірів (інтенції) та пошук способів та формування умов для їх реалізації у вигляді ланцюгів локальних дій;

– третій етап – формування команди та готовність до виконання дії, процесу її виконання на основі вибраних процедур з тактики і стратегії досягнення цільового стану;

– четвертий етап – післядія, яка виконується для оцінки результатів дій і їх порівняння з програмою, виявлення недоліків та оцінка якості виконання дій відносно цільової орієнтації.

При цьому виділяються чотири типи критеріїв співвідношення між ціле орієнтацією особи і ситуаційним станом:

– початковий стан;

– темп руху до цілі на основі наявних енергоресурсів;

– тип дії (в залежності від тактики і стратегії досягнення мети);

– емоційний, психічний стан, активність в досягненні і реалізації мети як кінцевого стану.

Кінцевий стан може мати нечітку розмиту ціль, невизначеність в часі і просторі. Інформація про поточний стан особи формується в перцептивному

вході процесора прийняття рішень і сприймається як:

– оцінка стану середовища;

– інформація про результати власних дій;

– інформація з внутрішнього стану цілеформуючої і цілеспрямовуючої системи;

– класифікація ситуації і формування правил дій на основі нечіткої діагностичної інформації.

Роль виявленого розходження поведінки особи відносно цілеорієнтації, полягає в селективності, у виборі можливих альтернатив та оцінці їх енергетичного рівня (потенціалу) у випадку необхідності зміни стану, тобто виступає як певний рівень, рід мотивації при досягненні мети в залежності від типу ситуації та рівня необхідних енергозатрат. Основні структурні блоки системи контролю цілеорієнтованих дій на досягнення визначеної мети ґрунтуються на теоретичних моделях психічної інтелектуальної регуляції поведінки [2–3, 6, 9]:

– хронологічні послідовності циклів інтелектуальних і фізіологічних дій;

– цикли контролю дій в напрямку досягнення мети (початок і кінець дії) на основі вибраних стратегій;

– інтенціональні процеси формування намірів, визначення цілі і програми дій;

– оціночні процеси і порівняння параметрів протікаючих дій з заданими згідно цільової орієнтації, їх класифікація і виконання управляючих дій згідно з програмою поведінки і мети;

Наявність різних рівнів реалізації процесів концентрації уваги підтверджується в нейрон-психологічних дослідженнях функціонування ієрархії мозкових структур (рис. 1).

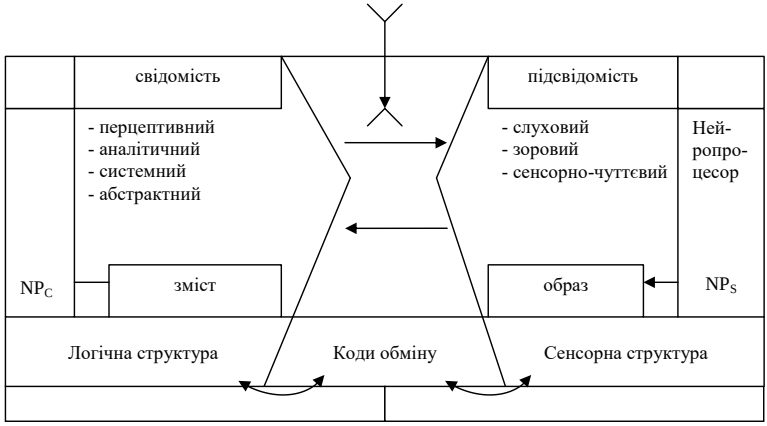


Рисунок 1 – Модель обміну інформації в нейроструктурі ієрархій мозку особи, де NP_C, NP_S – нейроструктури мозку для опрацювання логічної та сенсорної інформації.

Рівні опрацювання інформації в інтелектуальних системах (психологічний аспект) [1, 5, 8] визначають творчий і управлінський потенціал особи.

Концепція Крейка і Локхарта ієрархічної структури рівневої організації обробки даних (стимули, збурення, образи, звук) включає блоки обробки інформації при функціонуванні, яких використовуються наступні типи пам'яті:

– надкоротка оперативна слухова пам'ять;

– коротко часова оперативна просторова пам'ять;

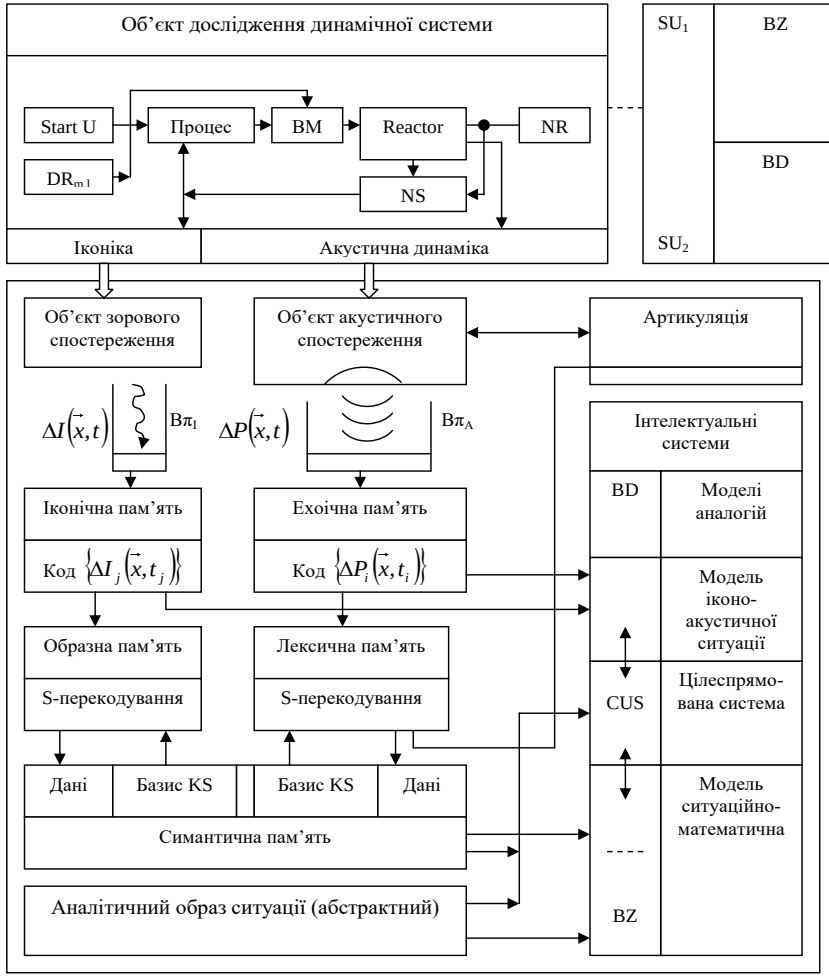


Рисунок 2 – Структурна схема ієрархії обробки даних в людино-машинних системах

– довго часова пам'ять на основі перетворень у вербально-символьний код образів понять, символів, структури об'єктів на базі симантичних моделей бази знань.

З точки зору цілеорієнтованого опрацювання даних, виділені такі рівні ієрархії в організації нейроструктури мозку особи-оператора: сенсорний рівень; лексичний рівень; образний рівень. Розглянемо структурну схему (рис. 2), на якій відображено рівні функціональної ієрархії при взаємодії людино-машинних систем в структурі АСУ-ТП різного призначення (енергетика, виробництво).

Висновки. На основі елементів теорії інтелекту та когнітивної психології розглянуто моделі прийняття рішень в людино-машинних інтегрованих системах. Це дає змогу обґрунтувати процедури тестування особи та оцінки її здатності до прийняття управлінських рішень в умовах нормальних й екстремальних ситуацій.

Інформаційні джерела

1. Орбан-Лембрик Л. Є. Психологія управління. К.: Академвидав. 2003. 548 с.

2. Ру Д., Сулье Д. Управління. К.: Основи. 1995. 447 с.

3. Дурняк Б. В., Сікора Л. С., Антоник М. С., Ткачук Р. Л. Автоматизовані людино-машинні системи управління інтегрованими ієрархічними організаційними та виробничими структурами в умовах ризику і конфліктів. Львів: Українська академія друкарства, 2013. 514 с.

4. Ткачук Р. Л., Сікора Л. С. Логіко-когнітивні моделі формування управлінських рішень інтегрованими системами в екстремальних умовах: посібник. Львів: Ліга–Прес, 2010. 404 с.

5. Дурняк Б. В., Сікора Л. С., Антоник М. С., Ткачук Р. Л. Когнітивні моделі формування стратегій оперативного управління інтегрованими ієрархічними структурами в умовах ризиків і конфліктів. Львів: Українська академія друкарства, 2013. 449 с.

6. Лиса Н. К., Сікора Л. С., Ткачук Р. Л., Тупичак Л. Л., Таланчук Р. Р., Федина Б. І., Федевич О. Ю. Інформаційні та когнітивні технології оцінки ситуації в автоматизованих системах управління в умовах дії завад і факторів збою. Комп'ютерні технології друкарства. 2020. № 1 (45). – С. 110–130. doi: 10.32403/2411-9210-2021-1-45-110-130. URL: https://ctp.uad.edu.ua/images//ktd/45_11.pdf.

7. Sikora L., Lysa N., Tkachuk R., Fedyna B., Fedevich O. Information and Cognitive Components of Knowledge Formation in Procedures for Assessing Dynamic Situations in Cyber-Physical // CEUR Workshop Proceedings. – 2022. – Vol. 3156 : proceedings of the 3rd International workshop on intelligent information technologies & systems of information security, Khmelnytskyi, Ukraine, March 23–25, 2022, pp. 129–139. ISSN1613-0073. (SciVerse Scopus). URL: https://ceur-ws.org/Vol-3156/paper7.pdf

8. Sikora L., Lysa N., Fedevych O., Navytka M., Tkachuk R., Dronyuk I. Information technologies of formation of intellectual decision-making strategies under conditions of cognitive failures. CEUR Workshop Proceedingsthis link is disabled, 2020, 2805, pp. 233–254.

9. Sikora L., Lysa N., Dronyuk I., Fedevych O., Tkachuk R., Talanchuk R. Information-resource and cognitive concept of threat's influence identification on technogenic system based on the cause and category diagrams integration. The 2nd International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS-2021), 2021, 2853, pp. 398–416.

УДК 621.3

МОДЕЛІ КООРДИНАЦІЙНИХ СТРАТЕГІЙ ПРИЙНЯТТЯ РІШЕНЬ В ІЄРАРХІЧНИХ КІБЕР ТЕХНОГЕННИХ СИСТЕМАХ

***Назарій ХИЛЯК*[1]**
***Наталія ЛИСА*[1]**
***Любов ТУПИЧАК*[1]**
***Олександра БОХАН*[2]**
***Михайло БОХАН*[2]**

[1]Національний університет "Львівська політехніка", м. Львів, Україна.
[2]Калуський політехнічний фаховий коледж, м. Львів, Україна.

Abstract. *In the article conception of construction of co-ordinating case frame is considered in the hierarchical system on the basis of procedure of concordance of aims in having a special purpose space.*

Keywords*: expert system, strategy, coordination, synthesis, hierarchy.*

Анотація. *В статті розглянуто концепцію побудови моделі координаційного управління в ієрархічній системі на основі процедури узгодження цілей в цільовому просторі.*

Ключові слова: *експертна система, стратегія, координація, синтез, ієрархія.*

Актуальність. На сучасному етапі розвитку технологічних систем є характерною ситуація, коли управляючі рішення приймаються на різних рівнях ієрархії, від автоматичного управління АСУ-ТП до оперативного-управляючим персоналом і координаційного керування вищою ланкою. При цьому вищі ланки не завжди мають відповідний рівень професійної і спеціальної підготовки, а також не розуміють змісту технологічних ситуацій при зміні режимів поставки енергетичних і матеріальних ресурсів та дії збурюючих факторів як зовнішніх так і внутрішніх. Особливо небезпечний є той фактор нерозуміння, що при виведенні технологічних процесів на граничні режими при застарілому обладнанні з пониженим експлуатаційним ресурсом, можуть виникнути аварійні ситуації [1]. Виходом з цієї ситуації є розроблення системи підтримки прийняття рішень (СППР) в структуру якої входять експерти системи, системи інтелектуальної обробки даних, інформаційно-вимірювальні системи для автоматичного наповнення баз даних.

Координованість локальних стратегій як засіб забезпечення гарантованого функціонування технологічних структур.

Координованість підсистем n-го рівня ієрархії визначає таку управлінську дію на підсистеми, яка заставляє їх узгоджено функціонувати згідно локальної мети (цілі) так, щоб вся система досягла поставленої мети. Оскільки системи нижнього рівня мають власні цілі, які можуть не співпадати з

цілями верхніх рівнів ієрархії, то можливе виникнення конфліктів за ресурси, стратегій управління, цілеорієнтації, що приводить до неможливості досягнути глобальну ціль [2]. Дії стратегічного координатора направлені на:

– декомпозицію глобальної цілі в локальні;

– узгодження стратегій досягнення цілей та термінів реалізації;

– узгодження розподілу ресурсів для всіх рівнів ієрархії;

– розподіл повноважень на прийняття рішень для кожного рівня ієрархії, та визначення пріоритетів;

– формування набору рангових критеріїв якості управління, пов'язаних з оптимізацією ризику, рівня витрат ресурсів, гарантіями досягнення мети.

Поняття координації пов'язане з процедурами прийняття цілеорієнтованих рішень та оцінкою успіху в досягненні мети, на основі декомпозиції проблемної задачі управління:

$$\exists \mathit{Strat}\,\mathrm{Dcom(PZ)}, \exists \mathrm{Strat\,RZ}_{\mathrm{U}}^{\mathrm{C_i}}(X); \forall \mathrm{t} \in \mathrm{T_m} \subset T_D;$$

$\exists \Pi_R : \forall (x, D_{RZ}), P(x, D_{RZ}) \overset{T_m}{\equiv} x_i$ є розв'язком *i*-ої задачі відносно цілі G_i за термінальний час при якому $X_i(t) \in W_c$. Тоді $\exists \gamma_k \subset \{U_k\}, \exists \mathrm{Strat_k}(U_k \mid C_i \mid T_D)$ які впорядковують послідовність задач $\left\{D_{RZ}^0, D_{RZ}^1, ..., D_{RZ}^m\right\}$, при $\gamma_k(t \mid T_m)$, $T_m - \min\limits_{T_D} T_u; t_{ui} \subset T_U$. Де Π_R – правило, алгоритм, розв'язання задачі; t – поточний час; $\mathrm{Strat\,RZ}_{\mathrm{U}}^{\mathrm{C_i}}(X)$ – стратегія розв'язання задачі; $\mathrm{T_m}$ – термінальний час; $\mathit{Strat}\,\mathrm{Dcom(PZ)}$ – стратегія декомпозиції задачі; T_D – допустимий час; γ_k – координуючий сигнал з набору управлінь; T_U – час управляючої дії; $\{U_k\}, D_{RZ}^i$ – розв'язувана задача; t_{ui} – час реалізації управління; W_c – цільова область; $\mathrm{Strat_k}(U_k \mid C_i \mid T_D)$ – стратегія координації управляючих дій U_k для досягнення цілі C_i.

Відповідно можна виділити класи сигналів згідно їх функційного призначення: $KL_j(S_i \mid_{i=1}^{n})$ класи сигналів від кожного рівня, які визначають стан об'єктів і страт нижнього рівня. $KL_j(\gamma_k \mid U_k)$ – класи управляючих сигналів, направлених з верхнього рівня на нижній, які формуються на основі результатів розв'язання поточних задач управління D_{RZ}^i.

Ефективність управління в ієрархічній системі ґрунтується на міжрівневій інтеграції та стратифікації.

Означення. Інтеграція – ієрархічне впорядкування при об'єднанні систем з ціллю впорядкування оперативного функціонування, підвищення ефе-

ктивності в досягненні мети. Відповідно координація взаємодіючих підсистем покращує спосіб досягнення цілі на всіх рівнях ієрархії, згідно стратегії досягнення мети на основі вибору процедури пошуку схеми розв'язання задачі управління.

Процедури пошуку схем розв'язання задачі управління

Задача знаходження розв'язків в цільовому просторі, спряженому з простором станів ґрунтується на пошуку відображень $(X \times T_m) \to (X \times T_D)$, для яких маємо:

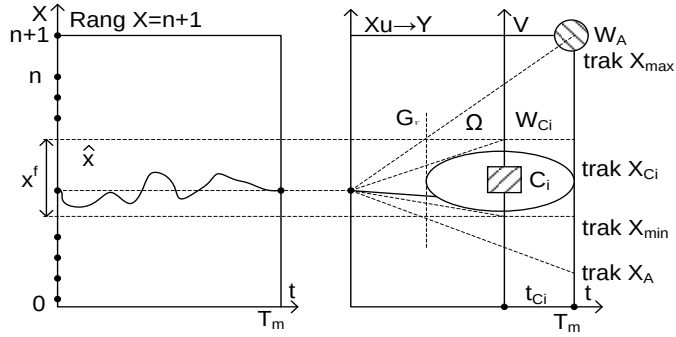
$$\begin{cases} g : x \to V, Rangx = n+1, \exists X^f, \exists \hat{x} \in X^f; \\ \forall x \in X^f : g(\hat{x}) \le g(x), \text{äå } G_p : x \to y, G_v : Y \to V_c \end{cases}$$

$X_{U_i}^{T_{m_i}}$ – множина всіх рішень для станів системи (об'єкта управління) при управлінні U_i і час T_{m_i}; X^f – множина допустимих рішень $X^f \subset X_U^{T_m}, X^f \notin W_A$; G – цільова функція ($G = G_p \otimes G_V$); W_A – аварійна область; V_c – плата за досягнення цілі в момент t_{C_i}; G_p – вихідна функція як модель процесу управління; G_V – функціонал якості управління; Ω – множина невизначеності стану об'єкту управління; F_τ – функція толерантності для якої маємо:

$$\forall (x, \omega) \in [X \times \Omega], \exists F_\tau;$$
$$G(x, \omega) \le F_\tau(\Omega), \tau : \Omega \to V$$

Отже маємо умову задовільного розв'язання задачі управління [3].

Відповідно будуємо простір станів і цільовий (рис. 1 а, б) на якому визначимо конус управляючих траєкторій.



а) Стан ОУ б) Цільовий простір

Рисунок 1 – Простори стану та цілі

Цільова функція може задаватись з врахуванням множини факторів впливу у вигляді відображень на цільовому просторі:

$$\left\{G_p : X \times \Omega \to Y, G_V : X \times \Omega \times Y \to V_C\right\} \mapsto \left\langle G(x,\omega) = G(x,\omega, G_p(x,\omega))\right\rangle$$

де $G()$ – цільова функція на Ω – невизначеності (структурної і параметричної), яка залежить від стратегії управління, проблемної ситуації і процедур прийняття рішень.

Система підтримки прийняття рішень

Означення $\left[S \subset X \times Y\right]$ називається системою підтримки прийняття рішень, якщо задано сімейство задач $\left\{ZD_x^i, x \in X\right\}_{i=1}^{m}$ з множини рішень Z і відображення $\left\{T : z_i \to Y, \forall x \in X, \forall y \in Y\right\}$, для якого маємо умову існування розв'язку $\exists z_i \in Z : ZD_x : T(z_i) = y, y \in C(C_i)$ – в просторі цілей системи $V(C_i) \subset Y \times T_{m_i}$ за термінальний час T_{m_i} – на основі схеми вибору стратегій $Strat\,\mathrm{R}(\mathrm{ZD_x} + T_D)$ які його забезпечують за допустимий час t (рис. 2).

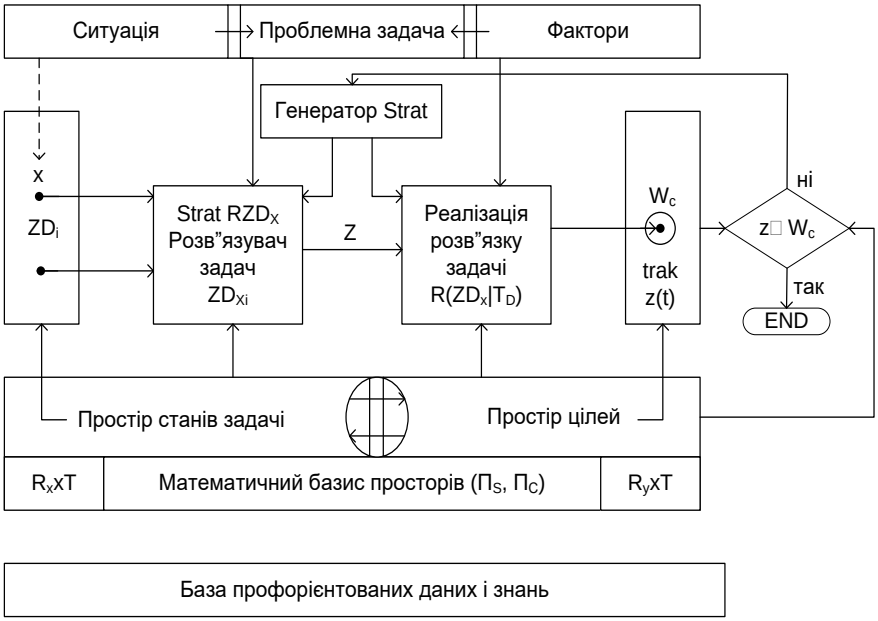


Рисунок 2 – Схема генерації стратегій розв'язання задач координаційного управління

Принцип координації стратегій в процедурах формування і прийняття рішень.

Множина інформаційних сигналів в ієрархічній системі розповсюджується як з верхніх рівнів на нижні (координація) (з $i \to i-m$ – рівні) так і з нижніх рівнів на верхні (з $i \to i+1...n$ рівні) (образ ситуації) та на *i*-рівні по горизонталі страти, і мають фіксовану змістовну – про стан об'єкта або управляючу команду, відповідно сигнали від верхнього рівня несуть координуючі управлінські рішення для нижньої страти.

Виділимо умови координації стратегій згідно цільових задач [4]:

– координованість ієрархічної системи до способу розв'язання глобальної проблемної задачі;

– узгодженість і сумісність цілей відносно стратегій координації для всіх рівнів;

– прогнозованість взаємодії всіх рівнів при вибраних стратегіях координації і управлінні;

– гарантованість успіху при мінімізації ризику конфлікту між рівнями.

Компоненти проблемної ситуації

Координація, як діяльність управляючої системи верхнього рівня, яка є цілеформуючою, пов'язана з типом розв'язуваних задач, які генерують ситуації: глобальні проблемні задачі, локальні для страт.

Відповідно, згідно мети системи, виконується процедура декомпозиції проблемної задачі на задачі верхнього і нижнього рівня, що, відповідно, пов'язано з наступними проблемами їх розв'язання. Розглянемо ці проблемні задачі згідно концепції координації Месаровича [5]:

I-проблема. Синтез координуючої системи. Якщо задано глобальну проблемну задачу, і процедура її декомпозиції на різні рівні, то необхідно знайти таку задачу, для якої існує спільна координуюча стратегія її розв'язання, на основі якої формуються управляючі сигнали для всіх рівнів:

$$\exists G(PZ \mid T_m \in T_D),\ \exists \Pi_R : D(PZ \to LZ_i \mid_{i=1}^{m}), \Pi_R \to StratU_i \mid C_i$$

II-проблема. Вибір методу, процедури, алгоритму координації. Якщо задана структура системи спряжена відносно цільової задачі, то необхідно знайти ефективний метод, алгоритм одержання (формування) координуючого сигналу, який би забезпечив узгоджену поведінку системи для досягнення мети:

$$(G(PZ_{C_i}) \leftrightarrow StruktISU) \mapsto \left[\exists (StratU \mid C_i \mid T_m) : Z_i \in W_c\right]$$

III-проблема. Модифікація стратегій Якщо ієрархічна система не координується відносно задачі $PZ(X \times T_m)$, то необхідно знайти таку модифікацію задачі, для якої існує координуюча стратегія:

$$\left\{\exists Strat(U \mid C_i \mid T_m) : Z_i \notin W_c\right\} \Rightarrow \Pi_R^K : (StratU_1 \xrightarrow{K} StratU_K)$$

IV-проблема. Декомпозиція глобальної задачі. Якщо сформульована тільки глобальна задача, то необхідно сформувати процедури розбиття на

класи задач верхнього і нижнього рівня, та, щоб стратегія їх розв'язання була координована відносно задачі верхнього рівня.

Якщо задача сформульована на вищому рівні ієрархії, то виникає проблема пошуку схеми її розв'язання, при цьому маємо два аспекти:

– пошук або генерація стратегії розв'язання задачі координаційного управління;

– синтез нової структури системи згідно цілей і стратегії координації, або модернізація і впорядкування існуючої системи згідно схеми, процедури розв'язання задачі.

Відповідно до цих умов будуємо схему вибору стратегій координації (рис. 3):

– згідно проблемної ситуації на і циклі формулюється проблемна задача;

– відповідно до принципу координації генеруються цільові задачі управління в ієрархії;

– перевіряється умова сумісності цілей і виконується вибір стратегій розв'язання задачі з бази знань та будується схема координаційного управління згідно рівнів ієрархії та типу структурної організації.

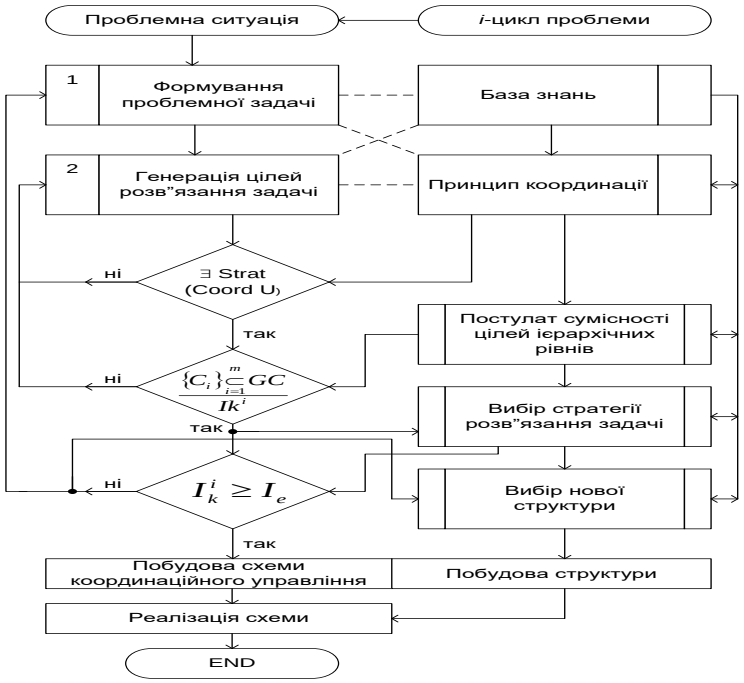


Рисунок 3 – Схема вибору стратегії координації для ієрархічної системи управління

Висновки. Розглянута концепція побудови моделі координаційного управління в ієрархічній системі на основі процедури узгодження стратегічних цілей з локальними цілями кожної страти. Показано, що процедура синтезу стратегій координацій буде ефективною якщо верхній рівень ієрархії управління буде керуватись управлінцями з високим професіоналізмом і інтелектуальною стійкістю, оскільки ці характеристики особи формуються на протязі довгих років підготовки, а ситуації кризові мають вибуховий характер, і тому командні вказівки приведуть систему в аварійний стан через нездатність верхнього рівня приймати ефективні рішення.

Інформаційні джерела

1. Ткачук Р. Л., Сікора Л. С. Логіко-когнітивні моделі формування управлінських рішень інтегрованими системами в екстремальних умовах: посібник. Львів: Ліга–Прес, 2010. 404 с.

2. Дурняк Б. В., Сікора Л. С., Антоник М. С., Ткачук Р. Л. Когнітивні моделі формування стратегій оперативного управління інтегрованими ієрархічними структурами в умовах ризиків і конфліктів. Львів: Українська академія друкарства, 2013. 449 с.

3. Сікора Л. С. Системологія прийняття рішень на управління в складних технологічних структурах. – Львів: Каменяр, 1998. – 453 с.

4. Сікора Л. С. Когнітивні моделі та логіка оперативного управління в ієрархічних інтегрованих системах в умовах ризику. Львів: ЦСД, 2009. 432 с.

5. Дурняк Б. В., Сікора Л. С., Антоник М. С., Ткачук Р. Л. Автоматизовані людино-машинні системи управління інтегрованими ієрархічними організаційними та виробничими структурами в умовах ризику і конфліктів. Львів: Українська академія друкарства, 2013. 514 с.

УДК 004.056.5:004.42

АНАЛІЗ БЕЗПЕКИ ПІДХОДУ “ІНФРАСТРУКТУРА ЯК КОД” (INFRASTRUCTURE AS CODE) В ХМАРНИХ ОБЧИСЛЕННЯХ

Богдан СКОРИНОВИЧ
Юрій КУЛИК
Володимир ГАВРИЛЯК
Національний університет “Львівська політехніка”, м. Львів, Україна.

Abstract. *The mechanism of infrastructure representation through code and key security challenges are considered. IaC security techniques aimed at reducing risks, ensuring configuration consistency, and increasing the stability of cloud infrastructure are presented.*

Keywords: *information security, infrastructure as code security, cloud computing security.*

Анотація. *Розглянуто механізм представлення інфраструктури через код та ключові виклики безпеки. Наведено методики забезпечення безпеки IaC, які спрямовані на зниження ризиків, забезпечення узгодженості конфігурацій та підвищення стабільності хмарної інфраструктури.*

Ключові слова: *інформаційна безпека, безпека інфраструктури "як код", безпека хмарних обчислень.*

Хмарні обчислення стали невід'ємною частиною сучасної IT-сфери, надаючи ряд переваг, таких як гнучкість, масштабованість та ефективність, порівнюючи з традиційними обчисленнями на фізичних машинах. Однак, отримавши ряд переваг, ми також отримали і значний недолік – зростання складності розгорнутих середовищ. Цей фактор створює нові виклики у сфері кібербезпеки для хмарних обчислень, які потребують вирішення. Підхід "Інфраструктура як код" (Infrastructure as Code, IaC) став ключовою практикою для забезпечення безпеки та стабільності хмарного середовища. Він дозволяє автоматизувати розгортання, конфігурацію та управління ресурсами, знижуючи ризики помилок та забезпечуючи узгодженість налаштувань.

Концепція "Інфраструктури як коду" тягне свої корені ще з 70-х років 20 століття, коли постала проблема керування та конфігурації наборами фізичних машин [1]. Світ інформаційних технологій зазнав значних змін з тих часів і теперішня інтерпретація та сприйняття даного поняття значно відрізняється від того, що малося на увазі в минулому, так як велика частина обчислень перейшли у хмарні середовища, а найпопулярнішою архітектурою розгортання додатків стали мікросервіси.

Але, незважаючи на ці зміни, проблема керування обчислювальними ресурсами залишається надзвичайно актуальною. Поняття обчислювальних ресурсів тут включає не тільки фізичні та віртуальні машини, а й великий спектр інших способів розгортання та запуску застосунків, такі як Docker, Kubernetes, безсерверні обчислення. Разом із цими ресурсами, концепція "Інфраструктури як коду" також активно використовується і до розгортання віртуальних мереж, сервісів зберігання даних, систем моніторингу, логування та багато чого іншого.

Узагальнюючи, застосування даного підходу актуальне до великої кількості різноманітних ресурсів, що, в кінцевому результаті, надає значні коротко- та довгострокові переваги:

– зменшення витрат часу на розгортання та підтримку інфраструктури;

– значне зниження ризиків людської помилки під час конфігурації ресурсів;

– уніфікованість створених середовищ;

– покращення безпеки за рахунок застосування стандартизованих конфігурацій.

Хоча переваги використання інфраструктури як коду (IaC) для хмарних обчислень є очевидними, впровадження даного підходу супроводжується певними викликами у сфері безпеки. До таких проблем варто віднести:

Недостатній рівень знань. Застосування інструментів IaC або конфігураційних шаблонів не усуває потреби у глибоких знаннях щодо управління хмарною інфраструктурою, налаштування ресурсів, тощо. *Наприклад* провайдери AWS та Azure пропонують понад 200 сервісів і їх кількість та методи конфігурації постійно змінюються. Недостатня компетенція та необдумане використання шаблонів можуть призвести до помилок, таких як створення користувачів з надмірними правами (IAM) або надання публічного доступу до обчислювальних ресурсів і сховищ даних.

Зберігання конфіденційних даних в конфігурації. Чутливі дані, такі як API-ключі, облікові дані або паролі, часто вбудовуються безпосередньо в IaC-файли, особливо на початкових етапах розробки. Це створює серйозні ризики, якщо такі файли зберігаються в системах контролю версій або випадково стають доступними для третіх осіб.

Некеровані зміни конфігурації. Коли ресурси залишаються активними, але не відстежуються чи не керуються за допомогою конфігурації (“примарні ресурси”), це створює розрив між бажаним станом (визначеним у коді) та фактичним станом інфраструктури. У результаті виникають проблеми неконтрольованого збільшення бюджетних витрат, створюються потенційні вектори атак і ускладнюється повна візуалізація хмарного середовища [2].

Вразливості залежностей. Конфігураційні скрипти часто залежать від зовнішніх модулів або бібліотек, які можуть мати власні вразливості, що залишаються непоміченими через відсутність належного моніторингу та валідації. Без регулярної перевірки та оновлення цих залежностей ризик компрометації систем значно зростає, оскільки потенційні вразливості можуть бути використані зловмисниками.

Недостатня захищеність файлів стану інфраструктури (State files). Файли стану, які використовуються інструментами IaC, зберігають детальну інформацію про поточний стан вашої інфраструктури, що може включати конфіденційні дані. Ці файли можуть зберігатися як віддалено, так і локально. Якщо ці файли неналежно захищені, несанкціонований доступ може призвести до розкриття конфігурацій ресурсів, маніпуляції інфраструктурою або втрати критичної інформації про стан.

Недостатнє забезпечення дотримання політик. Впровадження IaC може порушити існуючі робочі процеси, створюючи виклики для управління та стандартизації політик і архітектури. Без ефективного забезпечення дотримання політик розробники можуть ненавмисно розгортати небезпечні

або невідповідні конфігурації, вводячи вразливості безпеки та порушуючи нормативні вимоги.

Використання зловмисних шаблонів. Зловмисники можуть створювати шаблони конфігурації, які при розгортанні ініціюють ресурси, такі як EC2(віддалена обчислювальна машина), використовуючи шкідливі або підроблені образи. Ці образи можуть містити вбудоване шкідливе програмне забезпечення, бекдори або інший зловмисний код, що надає порушнику доступ до ваших систем. Такий несанкціонований доступ може призвести до витоку даних, несанкціонованої маніпуляції даними або служити відправною точкою для подальших атак у вашій мережі [3].

Для зниження ризиків IaC вимагає застосування комплексного підходу до забезпечення безпеки, що включає управління доступом, моніторинг, шифрування, автоматизацію перевірок і тестування [3]. У таблиці 1 систематизовані основні методики забезпечення безпеки IaC із коротким описом і прикладами інструментів, які допоможуть у реалізації кожного з підходів.

Цей підхід дозволяє не лише підвищити загальний рівень безпеки, але й зробити процес управління інфраструктурою прозорим, контрольованим і адаптованим до сучасних викликів.

Таблиця 1.

Основні методи забезпечення безпеки “інфраструктури як код” (IaC)

Метод	*Опис*	*Приклади інструментів/підходів*
Контроль змін та управління версіями	Відстеження, документування та контроль змін в IaC-коді. Захист стейт-файлів через шифрування, обмеження доступу та блокування одночасних змін.	Управління версіями: Git, GitLab, GitHub, Bitbucket Управління стейт-файлами: Terraform Cloud, AWS S3 + DynamoDB, Azure Storage Управління змінами: Atlantis, Terraform Enterprise, RunAtlantic
Статичний аналіз безпеки	Виявлення вразливостей у коді за допомогою автоматичних аналізаторів.	Хмарні провайдери: Checkov, CFRipper, AWS CloudFormation Guard Kubernetes/Containers: KICS, Kubesec Terraform: tfsec, Terrascan, Snyk IaC Загальні: SonarQube, Semgrep, Trivy
Автоматизація безпеки	Інтеграція перевірок та забезпечення безпеки в процеси розробки та розгортання інфраструктури.	CI/CD: Jenkins Security Plugins, GitLab Security Pipelines, GitHub Security Actions

Управління секретами	Безпечне зберігання та управління конфіденційними даними, такими як паролі, ключі API, сертифікати. Забезпечення безпечного доступу до секретів під час виконання.	Хмарні провайдери: AWS Secrets Manager, Azure Key Vault, GCP Secret Manage Kubernetes: Sealed Secrets, External Secrets Operator, HashiCorp Vault Універсальні: HashiCorp Vault, SOPS Container: Docker Secrets, Kubernetes Secrets
Тестування безпеки	Проведення регулярних перевірок безпеки інфраструктури, включаючи тестування на проникнення та оцінку вразливостей.	Infrastructure: InSpec, ServerSpec, Gauntlt Kubernetes: kube-hunter, kube-bench Containers: Clair, Dagda, Anchore Engine API/Serverless: OWASP ZAP, Burp Suite, Artillery
Відповідність вимогам (Compliance)	Забезпечення відповідності інфраструктури нормативним вимогам та галузевим стандартам безпеки.	Policy as Code: Open Policy Agent, Rego, Cloud Custodian Kubernetes: Kyverno, OPA Gatekeeper Стандарти: Chef Compliance, OpenSCAP Audit: Puppet Comply, Terraform Compliance
Управління доступом та ідентифікацією	Реалізація принципу найменших привілеїв, управління ролями та дозволами, забезпечення безпечної автентифікації.	Хмарні провайдери: AWS IAM, Azure AD, GCP IAM Kubernetes: RBAC, Open Policy Agent Універсальні: Okta, Auth0 Zero Trust: Istio, Consul, Spiffe/Spire

Висновки. Отже, забезпечення безпеки підходу “Інфраструктура як код” є критично важливо в умовах зростаючого використання хмарних обчислень. Дотримання вищезазначених методів дозволяє значно знизити ризики, забезпечуючи захист від можливих загроз під час застосування даної концепції та підвищуючи надійність хмарної інфраструктури.

Інформаційні джерела

1. Infrastructure as Code: Past, Present, Future. URL: https://www.infoq.com/presentations/iac-challenges-future/

2. Top 5 security concerns for infrastructure as code. URL: https://snyk.io/blog/top-5-security-concerns-iac/

3. Infrastructure as Code Security Cheatsheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/Infrastructure_as_Code_Security_ Cheat_Sheet.html

УДК 004.8

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ЗАХИСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УСТАНОВ ОСВІТНЬОЇ ГАЛУЗІ

***Ярослав ДОРОГИЙ*[1]**
***Василь ЦУРКАН*[2]**
***Олена ДОРОГА-ІВАНЮК*[3]**

[1]Донецький національний технічний Університет, м. Дрогобич, Україна.
[2]Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського, м. Київ, Україна.
[3]Пологівський ліцей Ковалівської територіального громади с. Пологи, Білоцерківський район, Київська обл., Україна.

Abstract. *The article examines the possibilities of using artificial intelligence (AI) technologies to protect critical infrastructure in the educational sector. Particular attention is paid to cyber threats caused by the military aggression of the Russian Federation and methods of countering them. Modern AI technologies are presented that can provide monitoring, threat identification and protection of sensitive data of educational institutions.*

Keywords: *educational sector, artificial intelligence, critical infrastructure, protection of critical infrastructure, cybersecurity.*

Анотація. *У статті розглянуто можливості застосування технологій штучного інтелекту (ШІ) для захисту критичної інфраструктури в освітній галузі. Особливу увагу приділено кіберзагрозам, зумовленим військовою агресією російської федерації, і методам протидії їм. Представлено сучасні технології ШІ, здатні забезпечити моніторинг, ідентифікацію загроз і захист чутливих даних освітніх установ.*

Ключові слова: *освітня галузь, штучний інтелект, критична інфраструктура, захист критичної інфраструктури, кібербезпека.*

Вступ. Критична інфраструктура освітньої галузі є ключовою для забезпечення стабільного функціонування освітніх установ і збереження даних студентів та працівників. З розвитком цифрових технологій зростає важливість захисту інформаційних ресурсів у зв'язку з посиленням кіберзагроз, особливо з боку країн, що використовують кіберпростір як засіб агресії. Однією з країн, що активно впроваджує кібернапади на освітні та інші установи України, є російська федерація. У цих умовах штучний інтелект може стати важливим інструментом для моніторингу і забезпечення безпеки освітньої інфраструктури.

Виклики для кібербезпеки освітньої галузі. З початком військової агресії рф проти України кількість кібератак на освітні установи країни значно зросла. Ці атаки часто спрямовані на порушення функціонування платформ для дистанційного навчання, що є важливою складовою освітнього процесу, особливо в

умовах війни. У той же час такі дії мають на меті викрадення конфіденційної інформації про учнів, студентів та працівників навчальних закладів.

Російські хакерські угруповання, зокрема ті, що пов'язані з державними структурами або діють з мовчазної згоди влади рф, цілеспрямовано атакують сервери українських освітніх установ. Основна мета цих атак – дестабілізація навчального процесу, знищення або спотворення критично важливих даних, що може порушити роботу установ і завдати шкоди особистій безпеці громадян. Такі кіберзлочини становлять загрозу для освітніх установ, оскільки вони підривають довіру до безпеки навчальних платформ, ускладнюють доступ до навчальних матеріалів, а також створюють ризики для особистих даних та інформації про академічні досягнення.

Ці кібератаки можуть також слугувати для впливу на інформаційний простір, підриваючи моральний стан студентства і викладачів та створюючи додатковий психологічний тиск на тлі військової агресії. З огляду на це, забезпечення захисту інформаційних систем освітньої галузі України стає стратегічно важливим завданням, для вирішення якого застосовуються передові технології, зокрема штучний інтелект, здатний забезпечити проактивний моніторинг, виявлення та відсіч подібним загрозам [1].

Застосування ШІ для моніторингу та виявлення загроз. ШІ здатний забезпечити постійний моніторинг мережевої інфраструктури навчальних закладів, що допомагає своєчасно виявляти й блокувати загрози. Системи на основі машинного навчання та обробки великих даних можуть розпізнавати патерни атак і аномальну активність, що можуть свідчити про спроби несанкціонованого доступу до систем [2]. Така технологія може бути особливо корисною для шкіл і університетів, які мають обмежені можливості в сфері кібербезпеки.

Захист чутливих даних за допомогою ШІ. Захист чутливих даних, зокрема інформації про студентів, їхню успішність та медичні дані, є однією з головних задач в освітній галузі. Використання ШІ значно покращує ефективність захисту таких даних. Алгоритми машинного навчання допомагають виявляти підозрілу активність, аналізуючи поведінку користувачів і їхні дії в реальному часі. Це дозволяє оперативно реагувати на спроби несанкціонованого доступу до чутливих даних або їх витоку, знижуючи ризики для студентів та викладачів. Важливим аспектом є те, що системи на основі ШІ можуть працювати в автоматичному режимі, що підвищує їхню ефективність порівняно з традиційними методами безпеки, де часто є потреба в людському втручанні.

Машинне навчання, зокрема методи класифікації документів та виявлення аномальних дій, можуть бути використані для захисту від витоків чутливої інформації в освітніх установах. *Наприклад*, системи, що використовують випадкові ліси (Random Forest), допомагають виявляти документи, які можуть містити конфіденційну інформацію, навіть якщо сама інформація не є очевидною на перший погляд [3].

Впровадження ШІ для підвищення кіберстійкості освітньої інфраструктури. Впровадження ШІ в освітній інфраструктурі може значно пок-

ращити її кіберстійкість, оскільки дозволяє виявляти вразливості та загрози на ранніх етапах. Зокрема, ШІ здатний автоматично здійснювати аналіз поведінки користувачів і виявляти аномалії, що є важливим для забезпечення безпеки систем дистанційного навчання. Інтеграція ШІ також дозволяє оперативно реагувати на атаки, автоматизувати процеси відновлення даних та адаптувати стратегії безпеки відповідно до нових загроз [4].

Висновки. Застосування штучного інтелекту в освітній галузі значно посилює захист критичної інфраструктури, особливо на тлі зростання загроз з боку рф. Використання інтелектуальних систем для моніторингу, виявлення аномалій, захисту чутливих даних та управління доступом дозволяє ефективніше боротися з кіберзагрозами та забезпечує стабільність навчального процесу.

Інформаційні джерела

1. Державна служба якості освіти України. Безпечне освітнє середовище – нові вимоги. SQE, 2023. URL: https://sqe.gov.ua/bezpechne-osvitnie-seredovishhe-novi-vim/

2. Pawlick J., Colbert E., & Zhu Q. “A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy”. Computers & Security, vol. 89, 2020, pp. 101–115. URL: https://doi.org/10.1016/j.cose.2019.101654.

3. Nightfall A. I. “How AI and Machine Learning Powers Next-Gen Data Leak Prevention (DLP)”. URL: https://www.nightfall.ai/blog/how-ai-and-machine-learning-powers-next-gen-data-leak-prevention-dlp.

4. Cyber Resilience for Critical Infrastructure Using AI. CPOMagazine. URL: https://www.cpomagazine.com/cyber-security/using-ai-to-build-cyber-resilience-for-critical-infrastructure/. [Accessed: 12-Nov-2024].

УДК 351.81

ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ ЗАКОНОДАВСТВА ЄС ДЛЯ ЕФЕКТИВНОГО ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ

***Ірина БЕРДИЧЕНКО*[1]**
***Ярослав ДОРОГИЙ*[1]**
***Олена ДОРОГА-ІВАНЮК*[2]**
[1]Донецький національний технічний Університет, м. Дрогобич, Україна.
[2]Пологівський ліцей Ковалівської територіального громади с. Пологи, Білоцерківський район, Київська обл., Україна.

Abstract. *Last year, a historic event took place – the European Council agreed to start negotiations on Ukraine’s accession to the EU. This process involves a set of systemic reforms, among the key ones – further adaptation of Ukrainian legislation to EU law. The financial sector is not left out of this activity. The priority areas are further implementation into national legislation of the provisions of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) [1] and alignment with the provisions*

of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2].

Keywords: *critical infrastructure, EU legislation, financial sector, critical infrastructure protection.*

Анотація. *У минулому році відбулася історична подія – Європейська Рада дала згоду розпочати перемовини про вступ України до ЄС. Цей процес передбачає комплекс системних реформ, серед ключових – подальша адаптація українського законодавства до права Євросоюзу. Фінансовий сектор не залишається осторонь у цій діяльності. Пріоритетними напрямками є подальша імплементація у національне законодавство положень Регламенту (ЄС) 2022/2554 про цифрову операційну стійкість для фінансового сектору (DORA) [1] та узгодження з нормами Директиви (ЄС) 2022/2557 Європейського парламенту та Ради від 14 грудня 2022 року про стійкість критично важливих суб'єктів і скасування Директиви Ради 2008/114/ЕС [2].*

Ключові слова: *критична інфраструктура, законодавство ЄС, фінансовий сектор, захист критичної інфраструктури.*

Вступ. Поточний стан національного законодавства свідчить про позитивні кроки, які відбулись впродовж останніх років у напряму підвищення ефективного забезпечення кібербезпеки та стійкості критичної інфраструктури, що було обумовлено, перш за все, гармонізацією з європейським законодавством.

Імплементація положень вищезгаданих правових актів ЄС знайшла своє відображення у таких законах нашої країні: "Про основні засади забезпечення кібербезпеки України" [3], "Про критичну інфраструктуру" [4], "Про захист інформації в інформаційно-комунікаційних системах" [5], "Про платіжні послуги" [6], "Про фінансові послуги та фінансові компанії" [7], а також низки рішень Уряду, серед іншого Стратегії кібербезпеки України [8].

Шляхи імплементації законодавства ЄС. Національний банк України, як регулятор банківської системи в Україні, а з 1 липня 2020 року – регулятор ринку небанківських фінансових послуг: страхових, лізингових, факторингових компаній, кредитних спілок, ломбардів та інших фінансових компаній, не залишається осторонь від євроінтеграційних процесів.

НБУ відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" є основним суб'єктом національної системи кібербезпеки України та організовує заходи із забезпечення кібербезпеки у фінансовому секторі, серед іншого, визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту для банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та на-

гляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг.

НБУ є одним із органів, який здійснює управління національною системою захисту критичної інфраструктури на загальнодержавному рівні та, водночас, виконує функції секторального органу у сфері захисту критичної інфраструктури фінансового сектору, і відповідно, наділений широким колом повноважень, визначених статтею 19 Закону України "Про критичну інфраструктуру".

Національним банком України забезпечено комплексний підхід до нормативно-правового врегулювання питань стосовно особливостей функціонування фінансового сектору, у тому числі, в умовах військової агресії російської федерації, забезпечення кіберстійкості та протидії кіберзагрозам, безперервності функціонування фінансового сектору, управління ризиками, що знайшло своє відображення не лише у вище перелічених законах, а і низці нормативно-правових актів НБУ, тут слід згадати про такі постанови Правління Національного банку: від 27.09.2017 № 95 "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі" [9], від 11.06.2018 № 64 "Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах" [10], від 12.08.2022 № 178 "Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України" [11] та інші.

Напрямок імплементації європейського законодавства у сфері забезпечення захисту критичної інфраструктури має високий рівень пріоритетності. На сьогоднішній день, законодавство України у цій сфері в значній мірі відповідає основним стандартам законодавства ЄС. Однак поряд з низкою позитивних змін існують деякі невирішені питання. Перш за все, необхідно передбачити впровадження європейського підходу до розуміння критично важливого суб'єкта та критичної інфраструктури.

Так, Директива 2022/2557 оперує поняттям критично важливого суб'єкту:

а) суб'єкт господарювання надає одну або декілька основних послуг;

б) суб'єкт господарювання здійснює діяльність і його критична інфраструктура розташована на території цієї держави-члена;

с) інцидент міг би мати значні руйнівні наслідки, як визначено відповідно до частини 1 статті 7, на надання суб'єктом господарювання однієї чи кількох

основних послуг або надання інших основних послуг у секторах, викладених у Додатку, які залежать від тієї чи тих основних послуг (стаття 6).

Тоді як критична інфраструктура – означає актив, об'єкт, обладнання, мережу чи систему або частину активу, об'єкта, обладнання, мережі чи системи, які необхідні для надання основних послуг (стаття 2 (4)).

У той же час, у національному законодавстві врегульовується захист об'єктів критичної інфраструктури, на відміну від європейського законодавства, у якому акцент на стійкість критично важливих суб'єктів.

Наступне, це імплементація положень статті 8 Директиви (ЄС) 2022/2557 стосовно критичних суб'єктів у банківській справі та інфраструктурі фінансового ринку (пункт 3 та 4 таблиці у Додатку до Директиви (ЄС) 2022/2557).

Стаття 8 визначає, що Держави-члени повинні гарантувати, що стаття 11 та розділи III, IV та VI не застосовуються до критичних суб'єктів, які вони визначили у секторах, зазначених у пунктах 3 та 4 таблиці у Додатку. Держави-члени можуть приймати або зберігати положення національного законодавства для досягнення більш високого рівня стійкості для цих критичних суб'єктів, за умови, що ці положення відповідають чинному законодавству Союзу.

Отже, виходячи із положень цієї статті, мова йде про питання, присвячені співробітництву між державами-членами (стаття 11), стійкості критичних об'єктів (розділ 3), у тому числі оцінці ризиків критично важливих суб'єктів (стаття 12 розділу 3) та заходів щодо підвищення стійкості критичних об'єктів (стаття 13, розділ 3), а також стосовно критичних суб'єктів, що мають особливе європейське значення (розділ IV), а саме виявлення критичних суб'єктів, що мають особливе європейське значення (стаття 17) – ті, що надають ті ж чи аналогічні основні послуги шести або більше державам-членам, і нарешті стосовно питань організації перевірок компетентними органами критичної інфраструктури (розділ VI).

Водночас, стаття 9 цієї Директиви визначає, що кожна держава-член призначає або засновує один або більше компетентних органів, відповідальних за правильне застосування та, у разі необхідності, виконання правил, викладених у цій Директиві, на національному рівні. Що стосується критично важливих суб'єктів у секторах, зазначених у пунктах 3 та 4 таблиці у Додатку до цієї Директиви, компетентними органами, в принципі, є компетентні органи, зазначені у статті 46 Регламенту (ЄС) 2022/2554. Держави-члени можуть призначити інший компетентний орган для секторів, зазначених у пунктах 3 та 4 таблиці в Додатку до цієї Директиви відповідно до існуючих національних рамок.

Отже, виходячи із зазначеного, норм статей 8 та 9 Директиви (ЄС) 2022/2557 доцільно імплементувати в частині визначення регуляторів фінансового ринку України, як компетентних органів в розумінні європейського законодавства.

Висновки. Імплементація положень Регламенту (ЄС) 2022/2554 про цифрову операційну стійкість для фінансового сектору (DORA) та узгодження з нормами Директиви (ЄС) 2022/2557 Європейського парламенту та Ради про

стійкість критично важливих суб'єктів і скасування Директиви Ради 2008/114/ЕС дозволить забезпечити комплексний підхід до забезпечення захисту критичної інфраструктури фінансового сектору та створити ефективну вітчизняну систему моніторингу й оцінки, яка відповідає європейським традиціям у сфері захисту критичної інфраструктури, що в свою чергу, потребуватиме змін до Закону України "Про критичну інфраструктуру" та окремих кореспондуючих змін до таких законів, як: "Про основні засади забезпечення кібербезпеки України", "Про банки і банківську діяльність", "Про фінансові послуги та фінансові компанії", "Про Національний банк України".

Інформаційні джерела

1. Регламент (ЄС) 2022/2554 про цифрову операційну стійкість для фінансового сектору (DORA) (онлайн). URL: http://surl.li/efowfn (дата звернення: 16 листопада 2024).

2. Директива (ЄС) 2022/2557 Європейського парламенту та Ради від 14 грудня 2022 року про стійкість критично важливих суб'єктів і скасування Директиви Ради 2008/114/ЕС (онлайн). URL: http://surl.li/rkfxey (дата звернення: 15 листопада 2024).

3. Про основні засади забезпечення кібербезпеки України: Закон України, 5 жовтня 2017 року, № 2163-VIII / Верховна Рада України (онлайн). URL: http://surl.li/ouqbyp (дата звернення: 15 листопада 2024).

4. Про критичну інфраструктуру: Закон України, 16 листопада 2021 року, № 1882-IX / Верховна Рада України (онлайн). URL: http://surl.li/daxfsm (дата звернення: 15 листопада 2024).

5. "Про захист інформації в інформаційно-комунікаційних системах": Закон України, 5 липня 1994 року, № 80/94-ВР / Верховна Рада України (онлайн). URL: http://surl.li/jeioai (дата звернення: 16 листопада 2024).

6. "Про платіжні послуги": Закон України, 30 червня 2021 року, № 1591-IX/ Верховна Рада України (онлайн) URL: http://surl.li/nhzsye (дата звернення: 15 листопада 2024).

7. "Про фінансові послуги та фінансові компанії" Закон України, 14 грудня 2021 року, № 1953-IX / Верховна Рада України (онлайн). URL: http://surl.li/yrieuc (дата звернення: 16 листопада 2024).

8. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" (онлайн). URL: http://surl.li/cbyycs (дата звернення: 15 листопада 2024).

9. Постанова Правління Національного банку України від 27.09.2017 № 95 "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі" (онлайн). URL: http://surl.li/xyjkbp (дата звернення: 15 листопада 2024).

10. Постанова Правління Національного банку України від 11.06.2018 № 64 "Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах" (онлайн). URL: http://surl.li/xhfnpy (дата звернення: 15 листопада 2024).

11. Постанова Правління Національного банку України від 12.08.2022 № 178 "Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України" (онлайн). URL: http://surl.li/tmlkke (дата звернення: 15 листопада 2024).

УДК 004.056

БЕЗПЕКА БЛОКЧЕЙН: АНАЛІЗ АТАК ТА ВРАЗЛИВОСТЕЙ

Максим СОРОЧЕНКО
Тетяна ЛАВРИК
Сумський Державний Університет, м. Суми, Україна.

Abstract. *This paper analyzes potential attacks on blockchain systems and explores vulnerabilities that can lead to security compromise. The main attack mechanisms are considered, including attacks on consensus mechanisms and smart contracts. Recommendations for improving the security of blockchain systems are proposed.*
Keywords: *blockchain, Sybil attack, 51% attack, smart contract vulnerabilities, security.*

Анотація. *У цій роботі проведено аналіз потенційних атак на блокчейн-системи та досліджено вразливості, які можуть призвести до компрометації безпеки. Розглянуто основні механізми атак, включаючи атаки на консенсусні механізми та смарт-контракти. Запропоновано рекомендації щодо підвищення рівня безпеки блокчейн-систем.*
Ключові слова: *блокчейн, атака Sybil, атака 51%, вразливості смарт-контрактів, безпека.*

Блокчейн як інноваційна технологія стала ключовим елементом у багатьох галузях, включаючи фінанси, логістику, медицину тощо. Широкий спектр публікацій щодо технології блокчейн віддзеркалює різноманітні аспекти її застосування, переваги та недоліки. Однак, відзначається необхідність подальших досліджень, зокрема, в аспекті виявлення та аналізу вразливостей, які можуть виникати у процесі використання блокчейн. Аналіз цих загроз та вразливостей є важливим для розуміння потенційних ризиків та розробки ефективних методів захисту.

Умовно можна розподілити вразливості, які можуть призвести до компрометації безпеки блокчейн, на три групи: технічні, інфраструктурні та людські.

Технічні вразливості – це такі, що пов’язані з помилками у реалізації алгоритмів, протоколів або коду блокчейну. Вони можуть містити недоліки у криптографічних алгоритмах, помилки у реалізації смарт-контрактів або недоліки у мережевих протоколах.

Інфраструктурні вразливості – це такі, що пов’язані з мережевою архітектурою блокчейну, фізичною інфраструктурою, що забезпечує його роботу, а також з інфраструктурними компонентами мережі, такими як вузли, гаманці, мережеві вузли тощо. *Наприклад*, недоліки у програмному забезпеченні вузлів, несанкціонований доступ до гаманців або вразливості мережевої інфраструктури.

Людські вразливості – це такі, що пов’язані з помилками, недоліками знань або навичок користувачів та розробників, а також соціальні маніпуля-

ції. *Наприклад*, слабкі паролі, неправильна конфігурація системи або психологічний вплив на співробітників для отримання конфіденційної інформації.

Крім цього, слід окремо відзначити і вразливості протоколу консенсусу, який є ключовим елементом блокчейну, що забезпечує узгодженість між децентралізованими вузлами мережі. До них відносять атаку 51 % та атаку Sybil. Атака 51% передбачає, що зловмисники отримують контроль над більшістю обчислювальної потужності мережі, що дає змогу маніпулювати транзакціями, здійснювати подвійні витрати та блокувати нові транзакції. Яскравим прикладом є атака на блокчейн Bitcoin Gold у 2018 році, де зловмисники змогли викрасти понад $18 мільйонів через подвійні витрати [0]. Атака Sybil передбачає створення зловмисником численних фальшивих вузлів для отримання контролю над мережею та впливу на процеси прийняття рішень. Це призводить до можливості викривлення консенсусу та потенційної маніпуляції транзакціями.

Вразливості смарт-контрактів також є поширеними в блокчейн-системах. Смарт-контракти – це автоматизовані програми, що виконуються у блокчейні без посередників. Вони відрізняються від традиційних контрактів тим, що їх умови виконуються автоматично, без участі третіх сторін [0]. Це знижує ризик людських помилок та підвищує ефективність процесів, але водночас створює потенційні вразливості через можливі помилки у програмному коді. Вони значно полегшують процеси взаємодії, але мають певні вразливості:

1) Помилки в коді: недоліки в реалізації логіки контракту можуть призвести до витоку коштів чи компрометації безпеки. Знаковим прикладом є атака на DAO у мережі Ethereum у 2016 році, коли зловмисники використали помилку для викрадення значної кількості токенів [0].

2) Oracle атаки: смарт-контракти часто взаємодіють із зовнішніми джерелами даних (оракулами), які можуть бути вразливими. Якщо оракул надасть некоректну інформацію, це може спричинити небажані наслідки, включаючи виконання неправильних умов контракту [0].

Розуміння описаних вище вразливостей підкреслює необхідність розробки надійних механізмів захисту для блокчейн-систем, що допоможе зменшити ризики атак та забезпечити стабільність роботи мережі. Для запобігання зазначеним атакам і зменшення вразливостей блокчейн-систем, рекомендується дотримуватися таких пунктів:

– використовувати вдосконалені механізми консенсусу, що ускладнюють захоплення 51% обчислювальної потужності;

– підвищувати рівень перевірки нових вузлів у мережі для унеможливлення атак Sybil;

– проводити регулярний аудит смарт-контрактів, використовуючи спеціалізовані інструменти, такі як MythX, OpenZeppelin Defender та ConsenSys Diligence, та ретельно тестувати код перед його впровадженням [0];

– забезпечувати децентралізацію оракулів та перевіряти надійність джерел даних.

Висновки. Аналізуючи вразливості блокчейн-систем та потенційні загрози, можна зробити кілька важливих висновків. Технологія блокчейну, незважаючи на свої переваги, піддається значним ризикам, що можуть вплинути на її безпеку та надійність. Описані вразливості демонструють те, що навіть найсучасніші мережі блокчейну не є повністю захищеними від зловмисних дій, а помилки в коді чи використання ненадійних джерел даних можуть призвести до серйозних наслідків. З метою зменшення ризиків та підвищення рівня безпеки важливо впроваджувати комплексні стратегії захисту. Це включає постійне вдосконалення механізмів консенсусу, ретельний аудит та тестування смарт-контрактів, застосування надійних методів аутентифікації та шифрування, а також перевірку джерел зовнішніх даних. Тільки завдяки комплексному підходу можна забезпечити стійкість блокчейн-систем до атак та підвищити довіру до цієї технології у сучасному світі.

Інформаційні джерела

1. 51% Attack (Атака 51%) – що це і як працює? ProBitcoin.com.ua. URL: https://probitcoin.com.ua/51-attack.html

2. Що таке смарт-контракти і навіщо вони потрібні простими словами – ITstatti.in.ua. IT статті – інформаційний блог | Заробіток в інтернеті, інвестиції, бізнес, фінанси, реклама та інтернет – ITstatti.in.ua. URL: https://itstatti.in.ua/crypto/ 997-shcho-take-smart-kontrakti.html

3. Ethereum: десятиліття випробувань і тріумфів, із перспективним майбутнім попереду. MEXC. URL: https://www.mexc.com/uk-UA/learn/article/17827791517596

4. Blockchain Oracle – Що таке блокчейн-оракули і як вони працюють?. web3.0 – нове покоління інтернету вже настало! URL: https://www.web3.org.ua/blockchain-oracle-scho-tse-take/

5. Awosika E. How To Write Robust And Sustainable Smart Contracts | Consensys Diligence. Consensys Diligence. URL: https://diligence.consensys.io/blog/2023/09/how-to-write-robust-and-sustainable-smart-contracts/

УДК 004.056:351.86

КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ПРИНЦИП ФУНКЦІОНУВАННЯ ПІДРОЗДІЛУ

Станіслав ТУЛЬВІНСЬКИЙ

Черкаський науково-дослідний експертно-криміналістичний центр МВС України, м. Черкаси, Україна.

Abstract. *The conference paper theses focus on Ukraine's cybersecurity amid the war. They cover measures to protect critical infrastructure, including government networks, banking, and energy systems, as well as international cooperation, personnel training, and the application of advanced technologies to counter cyber threats and ensure the state's information security.*

Keywords: *cybersecurity, Infrastructure, cyber threats, information security.*

Анотація. *Тези доповіді присвячені кібербезпеці України в умовах війни. Описуються заходи захисту критичної інфраструктури, зокрема урядових мереж, банків і енергетичних систем, а також міжнародна співпраця, підготовка кадрів і застосування передових технологій для протидії кіберзагрозам та забезпечення інформаційної безпеки держави.*

Ключові слова: *кібербезпека, інфраструктура, кіберзагрози, інформаційна безпека.*

Кібербезпека України під час військових дій є не лише технічною проблемою, а й стратегічним аспектом національної безпеки. Метою цього дослідження є аналіз основних елементів кіберзахисту України у відповідь на численні загрози, які супроводжують повномасштабну агресію. У зв'язку з цим акцент зроблено на виявленні методів, які дозволяють зменшити вразливість критичної інфраструктури та забезпечити ефективну протидію атакам на інформаційні системи держави. В контексті повномасштабного вторгнення росії кібербезпека є не лише технічним завданням, але й стратегічним напрямом національної оборони, який вимагає комплексного підходу та координації на рівні усіх галузей влади та військових структур.

Одним із ключових завдань є захист критично важливих об'єктів, зокрема урядових мереж, енергетичних систем, банківських установ і стратегічних об'єктів інфраструктури. Оскільки кібератаки можуть завдати серйозної шкоди національній безпеці, на перший план виходить необхідність оперативного виявлення, аналізу і реагування на потенційні загрози. Поряд з цим, постає питання застосування передових технологій, які дозволяють забезпечити цілісність, доступність та конфіденційність критичних даних. Основою сучасних систем кіберзахисту є інтеграція програмних рішень для моніторингу трафіку, які аналізують поведінку даних у мережах та виявляють підозрілу активність, що може свідчити про намагання отримати несанкціонований доступ до конфіденційної інформації.

Ефективний кіберзахист потребує координації між урядовими органами, приватним сектором та міжнародними партнерами. У цьому контексті важливу роль відіграє обмін інформацією про новітні кіберзагрози, а також взаємодопомога у створенні спільних стратегій, спрямованих на підвищення рівня кіберзахисту на національному рівні. Зокрема, міжнародна координація забезпечує можливість оперативно реагувати на загрози та підвищувати стійкість критичної інфраструктури за рахунок підтримки партнерів у сфері інформаційної безпеки. Додатковим аспектом є міжвідомча співпраця на внутрішньодержавному рівні, що дозволяє покращити обмін інформацією і ресурсами між установами.

Ще одним важливим завданням є підготовка кваліфікованих кадрів, які здатні швидко та ефективно реагувати на кібератаки, забезпечуючи надійний захист інформаційних ресурсів. Навчання особового складу та розвиток практичних навичок для протидії кіберзагрозам є невід'ємною частиною кібербезпеки. Особлива увага приділяється формуванню у співробітників

навичок, необхідних для своєчасного виявлення та усунення потенційних загроз, а також застосуванню найкращих практик, які допомагають зберегти стабільність і функціональність інформаційних систем.

Сучасні засоби кібербезпеки передбачають використання ряду програмних рішень, орієнтованих на виявлення, запобігання і нейтралізацію кіберзагроз. Антивірусні програми здійснюють безперервний моніторинг системи, що дозволяє оперативно виявляти та блокувати підозрілі файли та програми, знижуючи ризик проникнення шкідливих елементів до мереж. Для ефективного реагування на інциденти кібербезпеки використовуються програмні рішення для миттєвого реагування та відновлення роботи систем. Це включає інструменти для ізоляції компрометованих систем, відновлення даних з резервних копій і відновлення нормальної роботи інфраструктури після атаки. Крім того, значною мірою програмні засоби для кіберзахисту включають системи управління доступом, які регулюють доступ до критичних ресурсів інформаційної системи та забезпечують ідентифікацію і автентифікацію користувачів.

Важливим компонентом є також програмне забезпечення для моніторингу і обробки подій безпеки, яке збирає, аналізує і агрегує дані про події з різних джерел, щоб вчасно реагувати на потенційні загрози. Ці інструменти допомагають забезпечити постійний контроль і реагування на кіберподії, зменшуючи ризики та зберігаючи безпеку інформаційних систем.

Антивірусне програмне забезпечення відіграє ключову роль у забезпеченні кіберзахисту, гарантуючи виявлення, блокування та видалення шкідливих програм і загроз для інформаційної безпеки [1]. Воно є необхідним інструментом для захисту комп'ютерних систем від вірусів, троянів, шпигунського програмного забезпечення та інших видів вірусів. Антивірус відстежує активність програм і файлів у реальному часі, аналізує їхню поведінку та порівнює сигнатури для виявлення аномалій і потенційних загроз. Крім того, антивірус забезпечує сканування системи на предмет вразливостей і можливих точок входу для зловмисників. Він допомагає підтримувати високий рівень захисту шляхом постійного оновлення своїх вірусних баз даних і програмних компонентів, що дозволяє виявляти нові загрози, які можуть виникнути.

Важливим елементом захисту є також фаєрволи, які регулюють доступ до мережі, ізолюючи критичні ресурси від потенційно небезпечного трафіку [2]. Крім того, вони дозволяють контролювати і аналізувати мережеві пакети відповідно до правил безпеки, зменшуючи ризик несанкціонованого доступу та витоку інформації. Основна функція полягає в фільтрації і моніторингу мережевого трафіку з метою блокування небажаних з'єднань і захисту від атак ззовні.

Для забезпечення всебічного захисту використовуються системи моніторингу подій безпеки, які збирають, обробляють та аналізують інформацію про активність у мережах. Такі системи забезпечують своєчасне виявлення потен-

ційних загроз та дозволяють вжити необхідні заходи для їхньої нейтралізації. Також використовуються інструменти для управління доступом до інформаційних систем, які гарантують ідентифікацію користувачів і запобігають несанкціонованим спробам отримати доступ до конфіденційних даних.

Висновки. Таким чином, кібербезпека є комплексним завданням, що включає координацію зусиль, сучасні технічні рішення, підготовку кадрів та міжнародне співробітництво. Забезпечення захисту інформаційної інфраструктури держави потребує узгоджених дій і впровадження кращих практик кібербезпеки. Основні висновки дослідження свідчать, що ефективний кіберзахист вимагає цілеспрямованої роботи, орієнтованої на стійкість критичних ресурсів, інтеграцію передових технологій і застосування комплексних підходів до захисту даних.

Інформаційні джерела

1. Calder A. (2020). The cyber security handbook: Prepare for, respond to, and recover from cyber attacks. IT Governance Publishing. ISBN 9781787782617.

2. Xu S., Qian Y., & Hu R. Q. (2023). Cybersecurity in intelligent networking systems: Fundamentals and applications. Wiley-IEEE Press. ISBN 9781119783917.

УДК 004.056

НУЛЬОВА ДОВІРА: ПРИНЦИПИ, ВИКЛИКИ ТА ВПРОВАДЖЕННЯ

Тетяна КОРОБЕЙНІКОВА
Ангеліна БОДАК
Дарина БОРОДЕНКО
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *The study analyzes the adoption of Zero Trust paradigm for securing corporate networks in the context of the proliferation of cloud technologies and other trends that have negatively affected the security of perimeter-based networks. The principles of ZTM, ZTA are described with reference to the NIST SP 800-207 standard, a comparison of models is provided, and best practices for ZTM implementation are identified.*

Keywords: *zero trust, cybersecurity, corporate networks, threat model, access control, segmentation, automation, continuous monitoring.*

Анотація. *У роботі проведено аналіз використання парадигми нульової довіри (Zero Trust) для захисту корпоративних мереж при розповсюдженні хмарних технологій та інших явищ, що негативно вплинули на захищеність мереж на основі периметрової моделі. Описано принципи ZTM, ZTA, використовуючи стандарт NIST SP 800-207, наведено порівняння моделей та ідентифіковано найкращі практики з провадження.*

Ключові слова: *Нульова довіра (Zero Trust), кібербезпека, корпоративні мережі, модель загроз, контроль доступу, сегментація, автоматизація, безперервний моніторинг.*

Вступ. Сучасні тенденції, зумовлені поширеним використання хмарних сервісів та переходом працівників на віддалену роботу, ставлять під сумніви безпеку корпоративних мереж на основі периметрової довіри. Потенційним рішенням проблеми є імплементація принципів і архітектури моделі нульової довіри (ZTM). Дана модель передбачає захист усіх мережевих ресурсів та заснована на ідеї, що довіра ніколи не гарантується.

Метою дослідження є аналіз підходів і технологій захисту інформаційних систем корпоративних мереж з акцентом на виявлення найефективніших рішень.

Методи проведення дослідження: аналіз наукових праць, присвячених теоретичній та практичній реалізації концепцій нульової довіри (Zero Trust), зокрема стандарту NIST SP 800-207. Основа методології полягає у порівнянні моделей периметрової безпеки із Zero Trust, з метою оцінки їх переваг і недоліків.

Наукова новизна: огляд та узагальнення найкращих сучасних практик захисту інформаційних систем корпоративних мереж, виокремлення переваг і недоліків їх реалізації, ідентифікація потенційних напрямків розвитку Zero Trust.

Практична цінність: використання результатів роботи для імплементації ZTM для створення захищених корпоративних мереж, що передбачають використання ефективних систем безпеки для захисту від внутрішніх та зовнішніх загроз.

Концепція Zero Trust стала об’єктом численних досліджень завдяки її ефективності. Зокрема, розглядаються її архітектура, динамічний контроль доступу, сегментація, однак, проблеми масштабування Zero Trust у великих організаціях залишаються актуальними.

1. Принципи Zero Trust: Zero Trust ґрунтується на принципі “нікому не довіряй за замовчуванням” і передбачає багатофакторну автентифікацію, безперервний моніторинг, динамічну авторизацію та сегментацію мережі. Головна мета цієї моделі – мінімізувати ризик несанкціонованого доступу шляхом суворої перевірки всіх суб’єктів і об’єктів, а також забезпечити контроль доступу на основі мінімальних привілеїв.

2. Порівняння моделей безпеки: У моделі захисту на основі периметра акцент робиться на ізоляції мережі шляхом обмеження зовнішнього доступу, тоді як Zero Trust зосереджується на захисті конкретних ресурсів, незалежно від їхнього розташування. У традиційних системах доступ часто надається на основі статичних політик, тоді як Zero Trust застосовує динамічний підхід у реальному часі, що враховує поведінкові атрибути та контекст середовища. Також Zero Trust підтримує автоматизоване управління ризиками та обов’язкове застосування мінімальних привілеїв.

3. Архітектура Zero Trust: Модель Zero Trust використовує архітектуру, яка забезпечує комплексний захист і сувору перевірку кожного запиту

доступу. Згідно зі стандартом NIST SP 800-207, ця архітектура передбачає управління доступом на основі динамічних політик, класифікації даних, шифрування та постійного моніторингу мережі. Усі ресурси організації розглядаються як потенційно ненадійні, незалежно від їхнього фізичного чи мережевого розташування. У традиційній площині керування ZTA точка прийняття рішень (PDP) поділяється на двигун політики (PE) і адміністратора політики (PA). PE оцінює довіру суб'єкта на основі даних з різних джерел і приймає рішення про надання доступу до ресурсів. Для забезпечення точності та оперативності контролю доступу необхідно автоматизувати процес оцінки довіри, динамічно оновлюючи її значення в реальному часі на основі зібраної інформації. Політика доступу (PA) забезпечує встановлення з'єднання між суб'єктом і ресурсом, ґрунтуючись на статичних і динамічних правилах, які визначаються модулями ядра ZTA. Динамічні модулі, такі як постійна діагностика (CDM), розвідка загроз та системи SIEM, забезпечують моніторинг у реальному часі та адаптацію політик.

4. Захист ідентичностей та ресурсів: У Zero Trust критичне значення надається захисту ідентичностей користувачів, пристроїв, програм і даних. Для цього застосовуються інвентаризація активів, динамічна авторизація додатків, а також політики мінімальних привілеїв. Мережі сегментуються, а кожна взаємодія в них перевіряється через механізми міжмережевих екранів, ізоляції хостів та управління потоками.

Процес автентифікації в ZTA включає як перевірку користувачів, так і пристроїв, використовуючи біометричні методи та автентифікацію фізичного рівня (PLA). Штучний інтелект дозволяє автоматизувати перевірки, мінімізуючи ризик підроблених ідентифікацій.

Суворий контроль доступу, безперервний моніторинг і оцінка ризиків гарантують, що до ресурсів отримують доступ лише авторизовані особи. Це дозволяє знижувати вплив атак, спричинених компрометацією пристроїв або облікових записів.

Основними труднощами впровадження Zero Trust є: складність модернізації існуючої інфраструктури, потреба в інтеграції динамічних політик та значні початкові витрати. Проте застосування цієї моделі є необхідним для підвищення рівня кіберзахисту, особливо в умовах сучасних загроз, що орієнтовані на обхід традиційних периметрових систем. Використанням застарілих систем, які покладаються на неявну довіру та не забезпечують контрольовану комунікацію між ресурсами. Під час переходу до Zero Trust Model (ZTM) виникають труднощі з оновленням архітектури, створенням автоматизованих політик безпеки та впровадженням динамічної ідентифікації й авторизації. Це потребує значних інвестицій та комплексного підходу для адаптації систем до мінливих умов і забезпечення надійного захисту ресурсів.

Рекомендації для впровадження: Для ефективного впровадження Zero Trust необхідно використовувати стандарти, такі як NIST SP 800-207, ство-

рити динамічну систему управління ідентичностями та доступом, впровадити постійний моніторинг ризиків, а також забезпечити класифікацію й захист даних на всіх рівнях.

Сучасний підхід Zero Trust Model (ZTM) передбачає сукупність людей, процесів і технологій для забезпечення безпеки. Ключовими аспектами є визначення ресурсів, що потребують захисту (дані, застосунки, пристрої, користувачі), аналіз комунікаційних каналів, використання мікросегментації (vNET, Hub&Spoke) та постійний контроль. Безпеку забезпечують динамічні політики, Continuous Access Evaluation (CAE) і поведінкова багатофакторна автентифікація (Behavioral MFA), яка аналізує унікальні патерни користувача. Технології, такі як безпарольна автентифікація, поєднання фізичних пристроїв і біометрії, підвищують захист. Сервіси Okta, Auth0, Azure Active Directory спрощують керування ідентичностями та доступом, інтегруючи динамічну безпеку.

Побудова сучасних корпоративних мереж змінюється, широко використовуються різноманітні хмарні сервіси та технології, а кіберзагрози стають все більш комплексним та складним явищем. Відповідно використання застарілої моделі захисту на основі периметру не здатне задовольнити питання безпеки інформаційних систем. Дана модель ґрунтується на існуванні внутрішньої, так званої контрольованої зони, де користувачі та ресурси можуть вільно пересуватись по мережі, а захист впроваджується тільки по периметру. На заміну запропонована новітня модель побудови інформаційних систем – безпека нульової довіри, що описується в стандарті NIST SP 800-207, опублікованому в серпні 2020 року.

*Кращі практики сучасного світу***.** Імплементація ZTA – тривалий та трудомісткий процес переходу від традиційної системи до новітньої. Перш ніж розпочати даний перехід корпораціям необхідно визначити площину захисту, тобто провести інвентаризацію всіх наявних ресурсів і технологій, систематизуючи їх за категоріями: дані, застосунки, активи, користувачі, сервіси, пристрої, тощо. Проведення подібного аналізу дає змогу ідентифікувати вже наявні можливості для захисту систем, а також виявити прогалини. Оскільки ресурси повинні взаємодіяти між собою, отже далі визначаються комунікаційні канали, що вже стають основою для побудови самого ZTA та політик безпеки. Надалі забезпечується безперервний контроль та оптимізація даних процесів.

Мікросегментація у площині нульової довіри є підходом для забезпечення безпеки мереж, що полягає у поділі інфраструктури на дрібні та ізольовані сегменти з метою контролю та обмеження трафіку. Дана методика реалізується технологіями vNET, віртуальними мережами. Таким чином, доступ до ресурсів однієї підмережі не гарантує доступ до ресурсів іншої, слідуючи принципам нульової довіри. Масштабованість досягається за допомогою конфігурування інформаційних каналів між віртуальними мережами, створюючи Peered Networks, та Hub&Spoke, де присутній арбітр для встановлення неявно заданого зв’язку.

Створення динамічних політик досягається розробкою інвентарю з індикаторів стану безпеки для збору всієї можливої інформації про стан ресурсів за методом Кіплінга та визначення відхилень від норми. Також тут використовуються сигнали систем виявлення вторгнень (IDS), систем керування захистом інформації (SIEM), оркестрація, автоматизація й реагування системи безпеки (SOAR). Технологія безперервної оцінки доступу (CAE), що виступає двигуном політик, є інноваційним підходом для прийняття рішень про завершення сесій між ресурсами. Передбачається реалізація сервісу видачі токенів сесії, що також виступає посередником при комунікації інших ресурсів та здатний перервати сесію при фіксуванні тих чи інших помилок і загроз.

Критичним елементом ZTA є ідентичності, контроль за ними пов'язаний з багатьма можливими впровадженнями, де важливу роль відіграє не тільки стан безпеки корпоративних систем, а також ефективність відносно кінцевих користувачів. Популярними методами автентифікації є: багатофакторна автентифікація, що складається з трьох аспектів (щось, що користувач знає, має та щось, чим користувач є); безпарольна автентифікація, де можуть використовуватись фізичні пристрої з підтримкою стандарту FIDO2, біометрія, одноразові паролі, push-повідомлення; поведінкова багатофакторна автентифікація, що використовує пасивну біометрію, аналізуючи дії користувача за поведінковими патернами його профілю. Також існують сервіси автентифікації, що дозволяють спростити керування ідентичностями та доступом, такі як: Microsoft Azure Active Directory, Okta, Auth0.

Висновок. Впровадження Zero Trust потребує глибокої модернізації інфраструктури, автоматизації політик доступу і пристосування до зростаючого навантаження на системи. Збільшення використання SaaS-додатків створює нові вразливості в цифрових ланцюгах постачання. Як перспективне рішення запропоновано використання динамічних ідентичностей, де посередники можуть забезпечувати безпечне з'єднання та контроль доступу, що сприяє зниженню ризиків у складних та динамічних мережах.

Інформаційні джерела

1. Zero Trust Architecture (ZTA): A Comprehensive Survey / [N. F. Syed, S. W. Shah, A. Shaghaghi та ін.]. // IEEE Access. – 2022. – No10. – С. 57143–57179.

2. Zero Trust Architecture [Електронний ресурс] / S. Rose, O. Borchert, S. Mitchell, S. Connelly // COMPUTER SECURITY. – 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

3. Zero Trust Implementation Guide [Електронний ресурс] // Google Services. URL: https://services.google.com/fh/files/misc/zt_implem_guide_ 800_27.pdf.

4. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO. – Львів: Видавництво Львівської політехніки, 2021. – 232 с.

5. A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology / [D. Li, Z. Yang, S. Yu та ін.]. // Future Internet. – 2024. – No16. – С. 320.

УДК 004.056:37.091.33

РОЛЬ НАВЧАННЯ СПІВРОБІТНИКІВ У ЗАПОБІГАННІ КІБЕРАТАКАМ

Віталій ТОКАР
Василь ЛУЧИК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The importance of training employees in the basics of cybersecurity as a key element of the strategy for protecting organizations from cyberattacks is considered. Particular attention is paid to the role of the human factor in the spread of threats such as phishing, social engineering and malware. The effectiveness of educational initiatives, including regular training, simulations and the use of artificial intelligence for adaptive learning, is analyzed. It is shown that systematic training reduces the number of incidents by 50–70%, minimizing financial losses and reputational risks. The importance of creating a cybersecurity culture for the long-term stability of organizations and their competitiveness in the market is emphasized.*

Keywords: *cybersecurity, human factor, phishing attacks, social engineering, personnel training, cybersecurity culture, training, artificial intelligence, economic feasibility.*

Анотація. *Розглянуто значення навчання співробітників основам кібербезпеки як ключового елемента стратегії захисту організацій від кібератак. Особлива увага приділяється ролі людського фактора у поширенні загроз, таких як фішинг, соціальна інженерія та шкідливі програми. Проаналізовано ефективність освітніх ініціатив, включаючи регулярні тренінги, симуляції та використання штучного інтелекту для адаптивного навчання. Показано, що систематичне навчання зменшує кількість інцидентів на 50–70%, мінімізуючи фінансові втрати та репутаційні ризики. Наголошено на важливості створення культури кібербезпеки для довгострокової стабільності організацій та їх конкурентоспроможності на ринку.*

Ключові слова: *кібербезпека, людський фактор, фішингові атаки, соціальна інженерія, навчання персоналу, культура кібербезпеки, тренінги, штучний інтелект, економічна доцільність.*

Сучасні організації все частіше стають жертвами кібератак, які несуть значні фінансові та репутаційні ризики. Одним із ключових способів зниження цих ризиків є навчання співробітників основам кібербезпеки. Розуміння базових принципів безпеки, знання про фішингові атаки та інші поширені загрози дозволяє працівникам ефективніше реагувати на потенційні загрози. Цей текст аналізує, чому навчання співробітників є важливою складовою стратегії кіберзахисту. Більшість кібератак базується на експлуатації людського фактора, *наприклад*, через фішингові листи або соціальну інже-

нерію. Навчання дозволяє співробітникам розпізнавати такі загрози та зменшувати ризик успішного проникнення. Людський фактор залишається одним із головних векторів атак для кіберзлочинців. За допомогою фішингових листів, соціальної інженерії або маніпуляцій зловмисники експлуатують недосвідченість користувачів. Навчання працівників допомагає розпізнавати ці загрози, мінімізуючи ризик успішного проникнення.

Наприклад, регулярні тренінги, симуляції фішингових атак і тести дозволяють працівникам у реальних умовах покращувати навички розпізнавання небезпечних ситуацій, що знижує вразливість організації. Навчання співробітників має бути частиною загальної культури кібербезпеки. Створення тренінгів, що зосереджуються на базових принципах кібербезпеки, політиках безпеки та поведінкових реакціях, дає змогу забезпечити проактивний підхід до захисту інформації. Особлива увага приділяється освітнім ініціативам щодо сучасних загроз, таких як складні фішингові схеми або атаки через соціальні мережі. *Наприклад*, навчання про верифікацію джерел та ознак фейкових сайтів дозволяє співробітникам уникати поширених помилок, які часто призводять до витоку даних. Сучасні організації впроваджують автоматизовані платформи та AI-інструменти для проведення навчання з кібербезпеки. Ці інструменти дозволяють створювати адаптивні курси та симуляції, які враховують прогалини в знаннях конкретних співробітників.

Наприклад, спеціалізовані платформи можуть моделювати атаки або оцінювати здатність персоналу реагувати на потенційні загрози в реальному часі. Крім того, завдяки використанню AI можна відстежувати прогрес співробітників та автоматично адаптувати навчальні матеріали до їхнього рівня знань. Регулярне навчання дозволяє не лише підвищити обізнаність співробітників, але й знизити витрати на ліквідацію наслідків кібератак. Освічені працівники здатні швидше ідентифікувати загрози, вчасно повідомити про них відповідні відділи та уникати помилок, які призводять до втрат даних або фінансових збитків. *Наприклад*, організації, що впровадили систематичні освітні програми, демонструють на 50–70% меншу кількість інцидентів, пов’язаних із фішинговими атаками. Це доводить, що інвестиції в освітні ініціативи значно зміцнюють загальний рівень кіберзахисту компанії. Навчання співробітників є не лише технічним, а й стратегічним підходом до кіберзахисту. Створення культури безпеки, інтеграція сучасних освітніх платформ і систематична перевірка знань дозволяють мінімізувати ризики, пов’язані з людським фактором, і захистити організацію від сучасних загроз. Це є важливою інвестицією у безпеку, яка забезпечує довгострокову стабільність і довіру як клієнтів, так і партнерів.

Інвестиції в навчання співробітників основам кібербезпеки дозволяють значно зменшити фінансові втрати, пов’язані з кібератаками. *Наприклад*,

організації, які впроваджують регулярні тренінги та освітні програми, фіксують до 70% менше інцидентів фішингових атак, що знижує витрати на усунення наслідків та відновлення даних. За даними аналітиків, середня вартість ліквідації наслідків одного кіберінциденту може перевищувати $4 млн, тоді як витрати на навчання співробітників у кілька разів менші. Профілактичні заходи окупаються, забезпечуючи організаціям економію ресурсів та збереження репутації.

Освічений персонал не тільки ефективніше захищає організацію від загроз, але й працює продуктивніше. Знання основ кібергігієни дозволяє працівникам уникати типових помилок, як-от відкриття шкідливих файлів чи посилань, що викликають збої у роботі систем. Завдяки меншій кількості інцидентів, пов'язаних із зловмисними діями, компанії витрачають менше часу на виправлення помилок і можуть зосереджуватись на бізнес-цілях. Інвестиції у навчання також сприяють формуванню впевненості співробітників у роботі з сучасними технологіями, що позитивно впливає на загальну ефективність бізнесу. Ефективність інвестицій у навчання проявляється у довгостроковій перспективі. Кібербезпека є не лише технічним, але й стратегічним фактором, що впливає на довіру клієнтів, партнерів та інвесторів. Організації, які демонструють проактивний підхід до навчання персоналу, здобувають конкурентну перевагу на ринку, адже їхні дані краще захищені. Крім того, потенційні репутаційні втрати через витік даних можуть бути значно дорожчими, ніж витрати на освітні програми. Таким чином, навчання кібербезпеки стає не лише інструментом захисту, але й економічно доцільним кроком для зростання та зміцнення бізнесу.

Висновки. Навчання співробітників є фундаментальним елементом запобігання кібератакам. Залучення персоналу до регулярних тренінгів, спрямованих на вивчення нових загроз, значно посилює загальний рівень захисту компанії. Ефективна програма навчання не лише підвищує кіберграмотність, але й мінімізує вплив людського фактора на безпеку організації. Простіше кажучи, інвестиції у навчання співробітників – це необхідний крок до створення надійного захисту у цифровому світі.

Інформаційні джерела

1. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України. URL: https://niss.gov.ua/sites/default/files/2018-06/AD_Dubov_206x301_pp1-84_press-b44d7.pdf (дата звернення: 14.11.2024).

2. Інформаційна безпека у 2024 році: які навички та сертифікації з кібербезпеки необхідні для успішної кар'єри. URL: https://www.h-x.technology/ua/blog-ua/essential-skills-careers-information-security-ua (дата звернення: 16.11.2024).

3. Кібербезпека в інформаційцному суспільстві. URL: https://ippi.org.ua/sites/default/files/2024-4.pdf (дата звернення: 15.11.2024).

УДК 004.056:005.8

КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

***Аліна ПОМАЗА-ПОНОМАРЕНКО*[1]**
***Дмитро ТАРАДУДА*[2]**

[1]Науковий відділ з дослідження проблем державної безпеки Національного університету цивільного захисту України, м. Черкаси, Україна.

[2]Кафедра організації та технічного забезпечення аварійно-рятувальних робіт Національного університету цивільного захисту України, м. Черкаси, Україна.

Abstract. *Ukraine and a significant part of the world are trying to implement measures at all levels of government aimed at protecting the cybersecurity of critical infrastructure facilities (hereinafter referred to as CIF). The growing number of cyberattacks on CIF in Ukraine and other countries of the world gives grounds to argue about the relevance of defining scientifically sound approaches to ensuring the effective functioning of the CIF cybersecurity system.*

Keywords: *critical infrastructure facility, cybersecurity, security and defense sector.*

Анотація. *Україна та значна частина країн світу намагаються реалізовувати заходи на всіх рівнях управління, спрямовані на захист кібербезпеки об'єктів критичної інфраструктури (далі – ОКІ). Зростаюча кількість кібератак на ОКІ в Україні та інших країнах світу дає підстави стверджувати про актуальність визначення науково виважених підходів до забезпечення ефективного функціонування системи кібербезпеки ОКІ.*

Ключові слова: *об'єкт критичної інфраструктури, кібербезпека, сектор безпеки та оборони.*

Система кібербезпеки ОКІ, яка має бути гнучкою й адаптивною [3–9], допомогти в чому може дієве інституційне забезпечення. Серед його складників можна виокремити суб'єктів, діяльність яких, з одного боку, спрямована на захист ОКІ, а з другого – на підтримку інформаційної та кібербезпеки. Одним із таких суб'єктів СБУ, що реалізує комплекс заходів із захисту ОКІ як одного з важливих елементів безпекової політики держави.

На виконання ст. 35 Конвенції Ради Європи про кіберзлочинність [1] у червні 2009 р. при СБУ було створено спеціальний підрозділу для боротьби з кіберзагрозами – Національний контактний пункт формату 24/7 із реагування та обміну терміновою інформацією про вчинені кіберзлочини. У 2012 р. у структурі СБУ також створили Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки (далі – ДКІБ СБУ). Він відповідає за стан державної безпеки в кібернетичній та інформаційній сферах, координує та контролює діяльність регіональних органів і підрозді-

лів центрального управління СБУ [2].

У 2015 р. у МВС розпочалось реформування його підрозділів у сфері боротьби з кіберзлочинністю шляхом створення Департаменту кіберполіції Національної поліції (далі – ДКП). ДКП створено сектор Національного контактного пункту з реагування на кіберзлочини, що здійснює інформаційно-аналітичне забезпечення органів державної влади про стан вирішення питань, що належать до його компетенції [2].

У Законі України "Про основні засади забезпечення кібербезпеки України" (2017 р.) [2, п. 19 ч. 1 ст. 1] визначено, що інформаційна та кібербезпека ОКІ передбачає функціонування комунікаційної або технологічної системи, кібератака на яку безпосередньо вплине на стале функціонування ОКІ. Захист від кібератак ОКІ здійснюється, зокрема, операторами таких об'єктів, а також підрозділами СБУ. Вони забезпечують кіберзахист: систем управління, каналів зв'язку, систем навігації та розвідки, банківських і фінансових систем, різних реєстрів та ін. елементів інформаційного середовища у сфері економіки, транспорту, енергетики, охорони здоров'я тощо, які забезпечують безпеку та оборону держави. Завдання СБУ у межах національної системи кібербезпеки визначені у п. 3 ч. 2 ст. 8 [там само].

У 2021 р. було схвалено Стратегію кібербезпеки України, у межах якої окреслено закономірності, відносини, взаємозв'язки, керівні засади, на яких ґрунтуються організація та здійснення кібербезпеки [2]. У межах цієї стратегії та Закону України "Про основні засади забезпечення кібербезпеки України" визначено суб'єктів забезпечення кібербезпеки: Президента України, Раду національної безпеки і оборони України, Національний координаційний центр кібербезпеки, Уряд України, Держспецзв'язку України, а також напрями координації зусиль між ними та сфери контролю (рис. 1). При цьому Держспецзв'язку України здійснює забезпечення урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA [там само, ст. 9]. Власник та/або керівник ОКІ організовує невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, а також відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки. Особиву роль покликаний також виконувати Національний координаційний центр кібербезпеки при РНБО що є загальнонаціональною координаційною структурою.

Слід відзначити, що в п. 3 ст. 8 Закону України "Про основні засади забезпечення кібербезпеки України" [2] наведено перелік різнохарактерних заходів, спрямованих на забезпечення функціонування національної системи кібербезпеки. У той же час, у законі не зазначено конкретного суб'єкта реалізації цих заходів. Такий підхід унеможливлює чітку персоніфікацію суб'єктів, що реалізують ті чи інші заходи, критерії їх виконання, рівень відповідальності того чи іншого суб'єкта тощо. Це, у свою чергу, вказує на

умовне виконання зазначених заходів щодо забезпечення кіберзахисту, у т.ч. ОКІ. На цій підставі вважаємо, що потребує доопрацювання даний закон у напрямку конкретизації суб'єктності реалізації 25 заходів із забезпечення функціонування національної системи кібербезпеки.

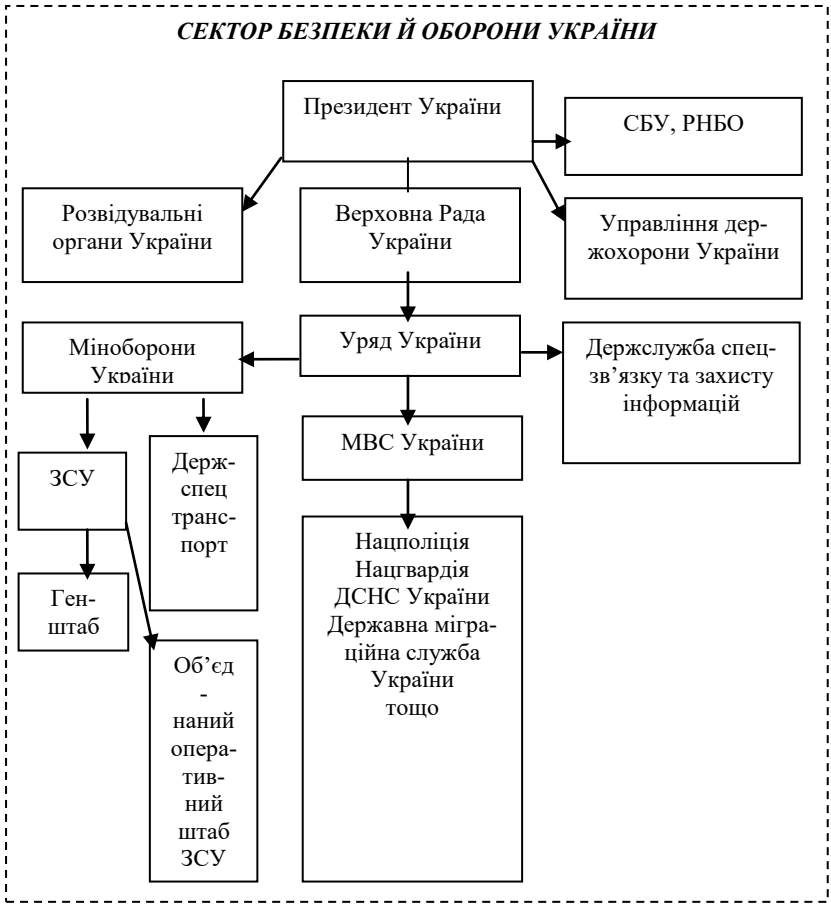


Рисунок 1 – Склад сектору безпеки й оборони України. Джерело: складено на підставі [2]

Висновки. Отже, протягом останніх років в Україні прийнято низку концептуальних нормативно-правових актів, у той же час, наявна проблема їх упровадження й узаємоузгодження, зокрема з міжнародними стандартами. Виявлено, що існує потреба в координуванні дій і взаємодії основних

суб'єктів кібербезпеки та кіберзахисту, зокрема у сфері захисту ОКІ, їх відповідності вимогам надійного й оперативного реагування на комплекс загроз в означеній сфері. Власне, потребує актуалізації діяльність Національного координаційного центру кібербезпеки при РНБО, що уповноважений узгоджувати й координувати діяльність правоохоронних органів, силових структур і відомств щодо протидії загрозам інформаційного та кіберпростору України, керувати проведенням комплексних навчань із забезпечення кібернетичної безпеки держави.

Інформаційні джерела

1. Лазор О. Я., Юник І. Г., Чемерпільська А. М. Організаційно-правові засади забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури України: формування та розвиток // Державне управління: удосконалення та розвиток. 2024. № 5. URL: https://www.nayka.com.ua/index.php/dy/article/view/3677/3712.

2. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1030-2022-%D0%BF#Text.

3. Помаза-Пономаренко А. Л., Тарадуда Д. В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об'єктах військово-промислового комплексу // Публічне адміністрування та національна безпека. 2024. № 3 (44). URL: https://www.inter-nauka.com/issues/administration2024/3/9732.

4. Помаза-Пономаренко А. Л., Тарадуда Д. В. Застосування цифрових технологій у сфері критичної інфраструктури для забезпечення цивільної безпеки // Матеріали Науково-практичної конференції "Інноваційні підходи до розвитку технологій та економіки" (27.06.2024 р., м. Свалява). 2024. – С. 248–251.

5. Помаза-Пономаренко А. Л., Тарадуда Д. В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об'єктах військово-промислового комплексу // Публічне адміністрування та національна безпека. 2024. № 3 (44). URL: https://www.inter-nauka.com/issues/administration2024/3/9732.

6. Помаза-Пономаренко А. Л., Тарадуда Д. В. Організація діяльності органів публічного управління щодо забезпечення цивільної безпеки на об'єктах підвищеної небезпеки України // Матеріали І Всеукраїнської науково-практичної конференції за міжнародною участю "Публічне управління та адміністрування в Україні: євроінтеграційний поступ" (31.05.2024 р., м. Івано-Франківськ). – С. 431–434.

7. Помаза-Пономаренко А. Л., Тарадуда Д. В. Роль технологій цифровізації в ідентифікації об'єктів підвищеної небезпеки в контексті забезпечення цивільної безпеки // Матеріали ІІІ Всеукраїнської науково-теоретичної конференції "Держава і суспільство: сучасні виклики та пошук рішень" (16.05.2024, м. Київ). – С. 337–340.

8. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // AD ALTA: Journal of Interdisciplinary Research. 2024. Vol. 14. Issue 1, pp. 216–220.

9. Popov O., Taraduda D., Sobyna V., Dement M., Pomaza-Ponomarenko A. (2020). Emergencies at Potentially Dangerous Objects Causing Atmosphere Pollution: Peculiarities of Chemically Hazardous Substances Migration. Systems, Decisions and Control in Energy I. Studies in Systems, Decision and Control. Switzerland: Springer International Publishing AG. Vol. 298, pp. 151–163.

УДК 004.056

КІБЕРБЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: СУЧАСНІ ВИКЛИКИ ТА РІШЕННЯ

Андрій ЩЕРБИНА
Національний університет Львівська політехніка, м. Львів, Україна.

Abstract. *The paper explores today's software cybersecurity challenges, including the rise of attacks, vulnerabilities and threats. Innovative solutions such as artificial intelligence, multi-factor authentication and DevSecOps are analyzed. Guidelines for developers and users to ensure security in the context of the proliferation of IoT, cloud technologies and quantum computing that are shaping the future of cybersecurity are discussed.*
Keywords: *cyber security, software, SSDLC, AI/ML, vulnerabilities, encryption.*

Анотація. *У роботі досліджуються сучасні виклики кібербезпеки програмного забезпечення, включаючи зростання атак, вразливості та загрози. Проаналізовано інноваційні рішення, такі як штучний інтелект, багатофакторна автентифікація та DevSecOps. Розглянуто рекомендації для розробників і користувачів щодо забезпечення безпеки в умовах поширення IoT, хмарних технологій і квантових обчислень, що формують майбутнє кібербезпеки.*
Ключові слова*: кібербезпека, програмне забезпечення, SSDLC, AI/ML, вразливості, шифрування.*

Вступ. Сьогодні програмне забезпечення (ПЗ) є основою роботи багатьох підприємств, урядових установ та приватного сектора. У зв'язку з активною діджиталізацією та глобальною інтеграцією інформаційних систем, питання кібербезпеки набуває критичного значення. Але одночасно, програмне забезпечення є потенційною мішенню для кіберзагроз, які можуть завдати суттєвої шкоди, починаючи від витоку конфіденційних даних і закінчуючи порушенням роботи цілих систем. У цьому контексті стає необхідним глибше розуміння сучасних викликів кібербезпеки, а також розробка рішень для ефективного захисту програмного забезпечення [1].

Мета дослідження сучасні виклики в сфері кібербезпеки програмного забезпечення для виявлення ключових загроз, з якими стикаються розробники та користувачі, а також запропонувати ефективні рішення для забезпечення безпечного функціонування програмних продуктів.

1. Проаналізувати основні сучасні кіберзагрози для програмного забезпечення, зокрема атаки типу "нульового дня", фішингові атаки, експлойти та зловмисне програмне забезпечення [2].

2. Оцінити вразливості, які найчастіше зустрічаються в програмних продуктах, і дослідити методи їх виявлення.

3. Розглянути сучасні підходи та інструменти для захисту програмного забезпечення, включаючи застосування шифрування, багатофакторної автентифікації, а також методів аналізу вихідного коду [3].

4. Дослідити роль штучного інтелекту та машинного навчання у виявленні загроз та автоматизації процесів забезпечення безпеки.

5. Розробити рекомендації для розробників та організацій щодо побудови безпечного середовища для роботи програмного забезпечення, включаючи інтеграцію безпеки на етапах розробки (DevSecOps).

6. Оцінити перспективи розвитку кібербезпеки програмного забезпечення в умовах нових викликів, таких як зростання IoT, хмарних технологій і квантових обчислень.

Отже, це нам дозволить сфокусувати дослідження на ключових аспектах кібербезпеки та запропонувати практичні шляхи вирішення актуальних проблем [4].

Основні виклики кібербезпеки програмного забезпечення:

Уразливості в коді, більшість кібератак спрямовані на експлуатацію помилок, допущених під час розробки програмного забезпечення. Типовими вразливостями є SQL-ін'єкції, міжсайтовий скриптинг (XSS), переповнення буфера тощо. Основними причинами таких проблем є [5]:

– неналежне тестування коду перед впровадженням;

– використання ненадійних сторонніх бібліотек або компонентів;

– відсутність автоматзованого аналізу безпеки під час розробки.

Соціальна інженерія. Зловмисники все частіше використовують психологічні методи маніпуляції для доступу до систем. Слабкі сторони у процесах автентифікації та недостатня обізнаність користувачів про загрози сприяють успішним атакам.

Розподілені атаки (DDoS) це атаки, спрямовані на виведення системи з ладу через перевантаження її ресурсів. Такі атаки стають дедалі складнішими через використання ботнетів та інших сучасних технологій.

Проблеми з управління оновленнями. Невчасне оновлення програмного забезпечення призводить до експлуатації вразливостей, відомих зловмисникам. Це особливо актуально для систем, які залежать від старих версій компонентів.

Сучасні рішення для кібербезпеки [1–3].

– Інтеграція безпеки у процес розробки.

– Розробка безпечного ПЗ має розпочинатися ще на етапі планування.

Використання методології Secure Software Development Lifecycle (SDLC) дозволяє включити безпеку на всіх етапах створення продукту. Це включає:

– Використання інструментів для статичного аналізу коду (Static Application Security Testing, SAST).

– Тестування під час виконання (Dynamic Application Security Testing, DAST).

– Регулярні пентести для виявлення вразливостей.

Шифрування даних. Забезпечення конфіденційності переданої та збереженої інформації є одним із основних заходів кібербезпеки. Сучасні крип-

тографічні алгоритми, такі як AES-256, SSL/TLS, забезпечують високий рівень захисту даних.

Багаторівнева автентифікація. Багатофакторна автентифікація (MFA) значно підвищує рівень захищеності облікових записів, вимагаючи підтвердження особи за допомогою кількох методів, таких як пароль, SMS-код чи біометричні дані.

Використання штучного інтелекту. Алгоритми машинного навчання можуть аналізувати поведінкові патерни користувачів, виявляти аномалії та запобігати потенційним атакам. *Наприклад*, такі системи можуть попереджати про підозрілу активність, як-от численні невдалі спроби входу.

Моніторинг і аудит. Постійний моніторинг мережі та додатків допомагає виявляти підозрілу активність у реальному часі. Регулярний аудит систем дозволяє своєчасно усувати вразливості.

Оновлення та патчі. Впровадження автоматизованих систем управління оновленнями допомагає уникнути ризиків, пов'язаних із застарілим програмним забезпеченням.

Перспективи розвитку кібербезпеки з огляду на швидкий розвиток кіберзагроз, необхідно розвивати такі напрямки:

– Квантова криптографія: розробка алгоритмів, стійких до атак квантових комп'ютерів.

– IoT-безпека: забезпечення захисту інтернет-речей, які часто стають мішенню атак через слабкі механізми автентифікації.

– Автоматизація безпеки: впровадження систем автоматичного виявлення та усунення вразливостей.

Висновки. Кібербезпека програмного забезпечення є складною, багатогранною проблемою, яка потребує комплексного підходу. Використання сучасних методологій розробки, інтеграція безпеки на всіх етапах життєвого циклу ПЗ та впровадження інноваційних рішень є ключем до протистояння кіберзагрозам. Успішна реалізація цих заходів сприяє не лише захисту ПЗ, але й підвищенню довіри користувачів до цифрових технологій, що є основою розвитку сучасного суспільства.

Інформаційні джерела

1. Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П. (2021).”Основи кіберпростору, кібербезпеки та кіберзахисту”: Навчальний посібник. Київ: Видавництво Ліра-К., 554.

2. Марущак О. І., Остроухов В. В., Присяжнюк М. М., Мельник Д. С. (2023). ”Організаційно-правові основи забезпечення кібербезпеки”: Навчальний посібник. Київ: Видавництво Ліра-К., 320.

3. Серія “Закони України” (2024).“Про захист персональних даних”: Закон: Видавництво Паливода А. В., 20.

4. Когут Ю. І., (2021). “Кібербезпека та ризики цифрової трансформації компаній”: Практичний посібник. Видавництво SIDCON, 372.

УДК 371:134

ГІГ-КОНТРАКТ, ЯК ПРАВОВЕ ПОЛЕ З ОХОРОНИ ПРАЦІ ДЛЯ ПРАЦІВНИКІВ ІТ-КОМПАНІЙ

Артем ІЩЕНКО
Володимир МАРИЧ
Кафедра промислової безпеки та охорони праці Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The latest legal instrument within the framework of Diya.City for flexible regulation of labor relations in the IT sphere. Gig contract provides for individualized terms of cooperation, social guarantees, optimization of taxation and protection of the interests of companies and employees, stimulating the development of the digital economy and innovations in Ukraine.*

Keywords: *labor protection, gig-contract, Diya.City, gig-specialists, IT-company.*

Анотація. *Новітній правовий інструмент у рамках Дія.City для гнучкого регулювання трудових відносин в ІТ-сфері. Гіг-контракт передбачає індивідуалізовані умови співпраці, соціальні гарантії, оптимізацію оподаткування та захист інтересів компаній і працівників, стимулюючи розвиток цифрової економіки та інновацій в Україні.*

Ключові слова: *охорона праці, гіг-контракт, Дія.City, гіг-спеціалісти, ІТ-компанія.*

В сьогоднішньому світі укладається різні види договорів та контрактів, що є важливою складовою формування правового поля між працівником та роботодавцем [1, 2]. Для працівників, які виконують трудову діяльність ІТ-компаніях доцільно використовувати унікальний правовий та податковий простір Дія.City [3, 4]. Цей простір відкриває нові можливості для бізнесу і працівників сфери ІТ, вводячи такі поняття, як резидент Дія.City, а також гіг-спеціаліст. Щоб стати резидентом, компанія має бути зареєстрована за українським законодавством, займатися кваліфікованими видами діяльності, відповідати умовам вступу та підготувати пакет документів. Кваліфіковані види діяльності: розробка та тестування програмного забезпечення, видання та розповсюдження Програмного забезпечення (ПЗ), зокрема SaaS, кіберспорт, навчання комп'ютерній грамотності, програмуванню, тестуванню та технічній підтримці ПЗ, кібербезпека, R&D в сфері ІТ і телеком, Digital Marketing та ads з використанням ПЗ, розробленого за участю резидентів, постачання послуг, пов'язаних з обігом віртуальних активів, робототехніка, розробка, запровадження та підтримка рішень міжнародних карткових платіжних систем, виробництво технологічних продуктів для використання в оборонній, промисловій та побутовій сферах, хостинг, зокрема хмарні датацентри, проєктування, виробництво безпілотні літаючі апарати (БПЛА), їх технічне обслуговування та ремонт, послуги з навчання керуванню БПЛА,

виготовлення, обслуговування, реалізація і ремонт біонічних протезів, протезів підвищеної функціональності та ортезів з комп'ютерним управлінням. Переваги, які компанія отримує від реєстрації це – низькі податкові ставки 5% ПДФО, ЄСВ 22% від мінімальної зарплати, 1,5% військовий збір, 9% на "виведений капітал" або 18% на прибуток [5].

Для стимулювання інвестицій: 0% на дохід фізосіб як дивіденди, які нараховані компанією-резидентом, за умови їх виплати не частіше 1 разу на 2 роки, податкова знижка: із загального оподатковуваного доходу віднімається сума, витрачена на придбання частки в українському стартапі [1, 2]. Також компанія-резидент сама обирає форму підписання виду трудового договору, а співпраця з ФОП, може підписати гіг-контракт, доступний тільки резидентам Дія.City. Гіг-контракти – цивільно-правовий договір, за яким гіг-спеціаліст зобов'язується виконувати роботи та/або надавати послуги відповідно до завдань резидента Дія Сіті як замовника, а резидент Дія Сіті зобов'язується оплачувати виконані роботи та/або надані послуги і забезпечувати гіг- спеціалісту належні умови для виконання робіт та/або надання послуг, а також соціальні гарантії [6].

Гіг-контракт укладається з будь-якою особою, яка укладає контракт з резидентом Дія.City. Якщо особо втрачає статус резедента гіг-контракт припиняє свою дію через три місяці. Результатом виконання гіг-контракту є оформлення актів виконаних робіт, які були прописані в контракті. Обсяг винагороди можна прописати погодинно так і за обсяг виконаної роботи. На гіг-спеціаліста не можна накладати штраф, лише у випадку пошкодження майна компанії або якщо цей випадок прописано в контракті [3, 4, 6].

Перевагою гіг-контракту від трудового договору – можливістю прописувати зарплату у валюті, але при сплаті податків вона буде переводитися за поточним курсом НБУ у національну гривню або за працю у вихідні потрійна або подвійна ставка, прописувати бонуси за перепрацювання, відпустки, декрет. ІТ-компанія матиме можливість захистити свої інтереси і одразу прописати права на інтелектуальну власність навіть при взаємодії на фріланс платформах. Також є розділення на компанії, що діють і стартапи, що дають можливість розвиватися малим компанія та спрощують оподаткування великим корпораціям [5].

Працівники мають можливість прописати кожен момент співпраці з роботодавцем, коли він планує йти у відпуску або робочий день розпочинається з одинадцятої години. Ще однією перевагою гіг-контракту для гіг-спеціаліста є тільки отримання заробітної плати за виконану роботу, а всі податки і трудові утримання оплачує роботодавець. Під час розірвання гіг-контракту, необхідно попередити іншу сторону за 30 і більше календарних днів, але строк повідомлення можна зменшити замінивши грошовою компенсацією. Також передбачено 3 місяці випробувального терміну, що надає можливість попередити про розірвання контракту за 3 дні. Ця система працює, як для роботодавця та і працівника.

Висновки. Гіг-контракт – інструмент, розроблений Міністерством цифрової трансформації для сприяння розвитку ІТ-компаній та оптимізації співпраці у технологічному секторі. Він формує правове підґрунтя з охорони праці для гнучкого регулювання трудових відносин, забезпечуючи баланс між інтересами роботодавців та працівників. Завдяки цьому механізму спрощується укладання угод, покращується правовий захист фахівців, а також стимулюється прозорість і ефективність ринку праці в цифровій економіці.

Інформаційні джерела

1. Машков К. Є., Горностай О. Б., Товт Т. О. Особливості трудових відносин в умовах воєнного стану: нормативно-правове регулювання Актуальні проблеми вітчизняної юриспруденції: збірник наукових праць. Дніпро, 2022. – №.1 – С.122–131.

2. Сарахман Х., Різник О., Горностай О. Дослідження впливу трудових ресурсів на економіку країни Охорона праці: освіта і практика. Проблеми та перспективи розвитку охорони праці: Збірник наук. праць ІІІ Всеукраїнської науково–практичної конференції викладачів та фахівців–практиків та ХІІІ Всеукраїнської науково-практичної конференції курсантів, студентів, аспірантів та ад'юнктів. – Львів: ЛДУ БЖД, 2023. – С. 123–125.

3. Постанова "Про визначення видів діяльності, здійснення яких стимулюється шляхом створення правового режиму Дія Сіті" від 13.08.2024 р. №467.

4. Постанова "Про внесення зміни до переліку видів діяльності, здійснення яких стимулюється шляхом створення правового режиму Дія Сіті" від 28.07.2023 №787.

5. Закон України "Про внесення змін до Податкового кодексу України щодо стимулювання розвитку цифрової економіки в Україні" від 14.12.2021 р. №1946-IX.

6. Закон України "Про стимулювання розвитку цифрової економіки в Україні" від 15.07.2021 р. №1667-IX.

УДК 004.93:658.14

ЗАХИСТ ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ШЛЯХОМ ВПРОВАДЖЕННЯ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ

Валентина ЯЩУК
Ростислав МИСЬКО
Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The current problem of protecting information assets in the face of growing cyber threats is discussed. The effectiveness of implementing integrated security systems (ISS) as a comprehensive solution for ensuring the security of information activities is studied. Modern threats such as cyberattacks, data leaks and disinformation are analyzed, and the need to transition from traditional protection methods to ISS is justified. The study demonstrates that ISS, combining physical, information and organizational security, allows for more effective detection, prevention and response to incidents. The main functions of*

ISS, such as monitoring, data analysis, forecasting and process automation, are described. The stages of ISS implementation are considered and examples of successful implementation in critical infrastructures are given.

Keywords: *integrated security system, cybersecurity, information security, data protection, cyberattacks, disinformation, artificial intelligence.*

Анотація. *Розглянуто актуальну проблему захисту інформаційних активів в умовах зростаючих кіберзагроз. Досліджується ефективність впровадження інтегрованих систем безпеки (ІСБ) як комплексного рішення для забезпечення безпеки інформаційної діяльності. Аналізуються сучасні загрози, такі як кібератаки, витоки даних і дезінформація, а також обґрунтовується необхідність переходу від традиційних методів захисту до ІСБ. Дослідження демонструє, що ІСБ, об'єднуючи фізичну, інформаційну та організаційну безпеку, дозволяє ефективніше виявляти, запобігати та реагувати на інциденти. Описано основні функції ІСБ, такі як моніторинг, аналіз даних, прогнозування та автоматизація процесів. Розглянуто етапи впровадження ІСБ та наведено приклади успішної реалізації в критично важливих інфраструктурах.*

Ключові слова: *інтегрована система безпеки, кібербезпека, інформаційна безпека, захист даних, кібератаки, дезінформація, штучний інтелект.*

Захист інформаційної діяльності набуває особливого значення в умовах цифровізації та глобалізації. Об'єкти інформаційної діяльності стикаються зі зростаючими загрозами, включаючи кібератаки, витоки даних та вплив дезінформації. Для ефективного протистояння цим викликам необхідно впроваджувати інтегровані системи безпеки (ІСБ), що поєднують фізичну та інформаційну безпеку в єдину інфраструктуру.

В умовах стрімкого розвитку цифрових технологій і глобальної цифровізації інформація стала одним із найцінніших ресурсів сучасного світу. Захист інформаційних об'єктів набуває стратегічного значення, оскільки навіть незначний витік даних може призвести до серйозних економічних, політичних або соціальних наслідків. Одним із ефективних рішень у цьому напрямку є впровадження інтегрованої системи безпеки (ІСБ), що поєднує технічні, організаційні та інформаційні засоби захисту.

Актуальність проблеми зумовлена зростанням кількості та складності загроз, пов'язаних із кібератаками, соціальною інженерією та витоками інформації. Відомо, що сучасні методи атак, включаючи використання штучного інтелекту (ШІ), значно ускладнюють процес виявлення та нейтралізації загроз. *Наприклад*, ШІ може бути використаний для автоматизованого пошуку вразливостей, генерації дезінформації чи створення фішингових атак, які здатні обійти навіть найсучасніші засоби захисту. Таким чином, традиційні методи захисту вже не забезпечують необхідного рівня безпеки, що робить впровадження інтегрованих рішень обов'язковим.

Інтегрована система безпеки поєднує фізичний захист, кібербезпеку та адміністративні заходи у єдину інфраструктуру, яка дозволяє своєчасно виявляти та усувати загрози. Однією з ключових переваг ІСБ є можливість централізова-

ного управління всіма елементами захисту, що забезпечує швидкість і ефективність реагування на інциденти. *Наприклад*, об'єднання систем відеоспостереження, контролю доступу та мережевих моніторингових інструментів дозволяє створити єдину картину стану безпеки об'єкта в реальному часі.

Основні функції ІСБ включають моніторинг і аналіз даних. Система збирає та аналізує інформацію з різних джерел для виявлення потенційних загроз. Також завдяки використанню ШІ ІСБ може прогнозувати розвиток подій та автоматично вживати заходів захисту. Автоматизація рутинних завдань дозволяє зосередити зусилля співробітників на вирішенні складніших проблем.

Процес впровадження інтегрованої системи безпеки включає кілька основних етапів. На першому етапі здійснюється аналіз ризиків, під час якого визначаються критичні точки, що потребують захисту. Наступним кроком є планування: розробляється концепція ІСБ, враховуючи специфіку об'єкта, його масштаби та потенційні загрози. Третій етап передбачає технічну реалізацію, яка включає встановлення апаратного та програмного забезпечення, інтеграцію систем і налаштування їх взаємодії. Четвертим етапом є навчання персоналу, яке включає інструктаж та тренінги для співробітників, відповідальних за експлуатацію системи. Завершальний етап – тестування та введення системи в експлуатацію з подальшим моніторингом її ефективності.

Важливим прикладом успішного впровадження ІСБ є інтеграція таких систем у критично важливих інфраструктурних об'єктах, як енергетика, транспорт або державні установи. Завдяки застосуванню передових рішень, що включають автоматизовані системи моніторингу, адаптивні алгоритми та засоби прогнозування, вдалося значно знизити ризики кібератак і забезпечити безперервність роботи.

Для підвищення ефективності інтегрованих систем безпеки важливо враховувати кілька ключових рекомендацій. По-перше, необхідно інвестувати в дослідження та розробки у сфері кібербезпеки, зокрема в створення адаптивних систем на основі ШІ. По-друге, слід регулярно проводити оновлення програмного забезпечення, щоб воно відповідало сучасним викликам. По-третє, важливим є навчання персоналу, яке забезпечить правильне використання технологій. Крім того, необхідно забезпечити правову базу, яка регулюватиме впровадження та використання таких систем.

Інтегрована система безпеки є ефективним рішенням для захисту об'єктів інформаційної діяльності. Вона забезпечує поєднання фізичного захисту, кібербезпеки та організаційних заходів, створюючи багаторівневу систему протидії загрозам. Успіх впровадження ІСБ залежить від комплексного підходу, інвестицій у сучасні технології та підвищення рівня обізнаності персоналу щодо безпеки.

Висновки. Підсумовуючи, можна зробити висновок, що інтегрована система безпеки є одним із найбільш ефективних підходів до захисту об'єктів інформаційної діяльності. Вона дозволяє значно підвищити рівень безпеки,

забезпечити безперебійну роботу систем та мінімізувати ризики, пов'язані з сучасними загрозами. Використання таких систем відкриває нові можливості для управління ризиками, що робить їх незамінними для сучасних організацій. Успішна реалізація ІСБ потребує комплексного підходу, який включає використання новітніх технологій, навчання персоналу та співпрацю на міжнародному рівні для обміну досвідом і розробки спільних стандартів.

Інформаційні джерела

1. ISO/IEC 27001:2013. "Information technology – Security techniques – Information security management systems – Requirements". Міжнародний стандарт із забезпечення інформаційної безпеки.

2. Барановський В. О. "Кібербезпека: основи та перспективи". Навчальний посібник. – Київ: КНУ імені Тараса Шевченка, 2021.

3. NIST Special Publication 800-53. "Security and Privacy Controls for Information Systems and Organizations". Національний інститут стандартів і технологій США, 2020.

4. Драб Ю., Ящук В. Основні підходи до побудови системи управління інформаційною безпекою. Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С. 29–32).

УДК 343.98:004.056

МЕТОДИ РОЗСЛІДУВАННЯ ТА ДОКУМЕНТУВАННЯ КІБЕРАТАК НА ДЕРЖАВНІ УСТАНОВИ

Данило ДРИШЛЮК
Василь ЛУЧИК

Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *Methods of investigation and documentation of cyber incidents targeting state institutions with critical information infrastructure are analyzed. Emphasis is placed on the importance of careful recording of electronic evidence in accordance with the current legislation of Ukraine and its use in legal proceedings. The role of artificial intelligence (AI) in detecting, analyzing and modeling cyber threats is analyzed, as well as its ability to automate routine tasks, reducing incident response time. The use of AI tools contributes to the rapid analysis of network traffic, detection of anomalies and documentation of cyber attacks, which is critically important for protecting national security. The problems of regulatory regulation are highlighted and recommendations are offered to improve the efficiency of cyber protection processes.*

Keywords: *cyberincidents, critical infrastructure, electronic evidence, artificial intelligence, network traffic, automation, cybersecurity, state institutions, recording of evidence.нотація.*

Анотація. *Проаналізовано методи розслідування та документування кіберінцидентів, спрямованих на державні установи з критичною інформаційною інфраструктурою. Акцент зроблено на важливості ретельної фіксації електронних доказів відповідно до чинного законодавства України та їх використання у судових процесах. Проаналізовано роль штучного інтелекту (AI) у виявленні, аналізі та моделюванні кіберзагроз, а також його здатність автоматизувати рутинні завдання, зменшуючи час реагування на інциденти. Використання AI-інструментів сприяє швидкому аналізу мережевого трафіку, виявленню аномалій та документуванню кібератак, що є критично важливим для захисту національної безпеки. Висвітлено проблеми нормативно-правового регулювання та запропоновано рекомендації щодо підвищення ефективності процесів кіберзахисту.*

Ключові слова: *кіберінциденти, критична інфраструктура, електронні докази, штучний інтелект, мережевий трафік, автоматизація, кібербезпека, державні установи, фіксація доказів.*

Кіберзагрози стають дедалі складнішими, особливо коли вони спрямовані на державні установи, що мають критичну інформаційну інфраструктуру. Для ефективного реагування та забезпечення кібербезпеки важливо розробляти й застосовувати сучасні методи розслідування й документування кібер інцидентів. Ці процеси мають бути ретельно регламентовані, оскільки вони не лише допомагають усувати наслідки атак, а й створюють підґрунтя для покарання винних.

Першим кроком у розслідуванні кіберінциденту є виявлення підозрілої активності в інформаційних системах. Для цього застосовуються спеціалізовані інструменти моніторингу, такі як системи аналізу журналів (log analysis tools) і аналізу мережевого трафіку. Ефективність цього етапу залежить від здатності ідентифікувати потенційні загрози, як-от спроби несанкціонованого доступу чи підозрілі дії користувачів. Однак недостатньо просто зафіксувати факт інциденту – важливо зрозуміти, чи він має злочинний характер і які саме порушення відбулися. У контексті українського законодавства ці дії є особливо важливими, адже цифрові докази мають відповідати вимогам допустимості для їх використання в суді. Після виявлення кіберінциденту необхідно оперативно локалізувати його, щоб мінімізувати подальші втрати або пошкодження систем.

На цьому етапі досліджуються вектори атаки – механізми, за допомогою яких зловмисники отримали доступ до системи. *Наприклад*, це може бути фішинговий лист, використання вразливості в програмному забезпеченні або викрадений пароль. Локалізація також включає ідентифікацію скомпрометованих систем і обмеження їхнього доступу до мережі. Як зазначають дослідники, недостатня нормативна база в Україні ускладнює цей процес, оскільки немає чітких інструкцій щодо обробки електронних доказів на цьому етапі. Ключовою складовою попереднього оцінювання є збір і фіксація електронних доказів, які можуть бути використані в розслідуванні. Ці

докази можуть включати журнали подій, знімки пам'яті, збережені файли, інформацію про мережеву активність і багато іншого. Відповідно до Закону України "Про електронні документи та електронний документообіг", електронні документи повинні мати відповідні реквізити для підтвердження їхньої автентичності. Проте, як зазначено в літературі, вітчизняне законодавство поки не повністю охоплює всі аспекти фіксації таких доказів, що може призводити до їхнього відхилення в судовому процесі.

На завершальному етапі попереднього оцінювання проводиться оцінка масштабу завданої шкоди. Це включає визначення обсягу втрачених даних, компрометації систем і потенційного впливу інциденту на бізнес або організацію. Важливо також зрозуміти, чи став кіберінцидент частиною більш масштабної злочинної діяльності, *наприклад*, організованих атак на національному чи міжнародному рівні. На основі зібраних даних складається попередній звіт, який лягає в основу подальших дій, таких як розробка заходів протидії або ініціювання кримінального провадження. У цьому контексті особливу увагу слід приділяти автентичності та надійності зібраної інформації, щоб забезпечити її доказову силу в суді.

AI-інструменти значно полегшують збір та аналіз великих обсягів даних під час розслідування кібератак. Вони використовують алгоритми для виявлення підозрілої активності в системах, аналізу логів та моніторингу мережевого трафіку. Завдяки автоматизації рутинних завдань, таких як класифікація інцидентів чи обробка доказів, AI допомагає спеціалістам зосередитися на складніших аспектах розслідування. *Наприклад*, інструменти аналізу журналів подій можуть швидко ідентифікувати, коли і як відбулася кібератака, що значно скорочує час на первинну оцінку інциденту.

AI-інструменти здатні розпізнавати шаблони, які можуть вказувати на кібератаку, *наприклад*, раптове збільшення трафіку або нетипову поведінку користувачів. Крім цього, автоматизація створення звітів дозволяє детально документувати інциденти. *Наприклад*, за допомогою служб транскрипції, таких як Transkriptor, аудіозаписи з інтерв'ю чи консультацій можуть бути перетворені на текстові документи для подальшого аналізу. Це підвищує точність і зменшує ризик помилок у критично важливій документації, що є основою для прийняття обґрунтованих рішень.

Під час розслідування кібератак на державні установи, AI допомагає ідентифікувати та попереджати нові загрози, що можуть становити небезпеку для національної безпеки. Інструменти на базі штучного інтелекту здатні моделювати сценарії атак, прогнозувати потенційні ризики та пропонувати рекомендації для їхньої мінімізації. *Наприклад*, автоматизований аналіз мережевого трафіку може виявляти кіберзагрози в реальному часі, дозволяючи реагувати на них ще до того, як вони спричинять значну шкоду. Це допомагає захищати конфіденційні дані, підтримуючи довіру громадян до державних структур.

Висновки. Використання AI-інструментів у розслідуванні кібератак значно підвищує ефективність роботи фахівців із кібербезпеки. Завдяки автоматизації трудомістких завдань, таких як пошук вразливостей або ідентифікація фішингових атак, скорочується час, необхідний для розслідування. Це не тільки економить ресурси, але й дозволяє оперативніше реагувати на загрози. Крім того, використання AI зменшує людський фактор у рутинних процесах, що знижує ймовірність помилок та сприяє більш обґрунтованим діям у межах забезпечення кібербезпеки.

Інформаційні джерела

1. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/03/27-1.pdf (дата звернення: 15.11.2024).

2. Виявлення та розслідування кіберзлочинів. URL: https://moodle.znu.edu.ua/pluginfile.php/1099287/mod_resource/content/1 (дата звернення: 16.11.2024).

3. Кібергігієна. Кібербезпека. Безпека держави. URL: https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf (дата звернення: 14.11.2024).

4. Штучний інтелект та протидія злочинності. URL: https://karchevskiy.com/2020/11/06/ai-vs-crime/ (дата звернення: 14.11.2024).

УДК 004.056:005

ВПЛИВ СУЧАСНИХ ЗАГРОЗ НА КІБЕРБЕЗПЕКУ ТА ЕФЕКТИВНІСТЬ ПІДХОДІВ ДО ЇХ ЗАПОБІГАННЯ

Олександр САФРОНОВ
Василь ЛУЧИК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article examines the current challenges of cybersecurity, driven by the evolution of threats such as malware, phishing, DDoS attacks, social engineering, and advanced persistent threats (APTs). It outlines the latest methods for protecting information assets, including zero-trust architecture, network segmentation, and the use of cloud technologies and artificial intelligence for anomaly analysis and real-time incident response. The human factor plays an important role and the need to train employees in the basics of cyber hygiene to reduce risks. The implementation of innovative approaches to cybersecurity is necessary to effectively counter personalized and complex attacks that are rapidly changing, especially in the context of the growth of remote workers and hybrid infrastructure.*

Keywords: *cybersecurity, modern threats, artificial intelligence, zero-trust architecture, cloud technologies, cyber hygiene, network anomalies, data protection.*

Анотація*. У статті розглянуто сучасні виклики кібербезпеки, зумовлені еволюцією загроз, таких як зловмисне програмне забезпечення, фішинг, DDoS-атаки, соціальна ін-*

женерія та вдосконалені постійні загрози (APT). Окреслено новітні методи захисту інформаційних активів, включно з архітектурою нульової довіри, сегментацією мережі, застосуванням хмарних технологій та штучного інтелекту для аналізу аномалій і реагування на інциденти в реальному часі. Важливу роль відіграє людський фактор та необхідність навчання співробітників основам кібергігієни для зниження ризиків. Впровадження інноваційних підходів до кібербезпеки є необхідним для ефективної протидії персоналізованим та складним атакам, що швидко змінюються, особливо в умовах зростання кількості віддалених працівників і гібридної інфраструктури.

***Ключові слова**: кібербезпека, сучасні загрози, штучний інтелект, архітектура нульової довіри, хмарні технології, кібергігієна, аномалії мережі, захист даних.*

У сучасному цифровому світі кібербезпека стає однією з найважливіших сфер захисту інформаційних активів, а зростання складності кіберзагроз ставить перед професіоналами нові виклики. Зловмисне програмне забезпечення, фішинг, DDoS-атаки, соціальна інженерія та вдосконалені постійні загрози (APT) змушують компанії застосовувати нові підходи до захисту своїх систем. Зі збільшенням кількості пристроїв, підключених до Інтернету, і використанням хмарних технологій ризик загроз значно зріс. Традиційні методи захисту, такі як антивірусні програми, брандмауери та системи виявлення вторгнень, поступово стають менш ефективними, оскільки кіберзлочинці використовують сучасні технології та методи для обходу заходів безпеки. На цьому тлі з'являються нові підходи, такі як архітектура нульової довіри, сегментація мережі та штучний інтелект для аналізу загроз, щоб забезпечити більш ефективну відповідь на сучасні виклики.

Актуальність даної теми зумовлена постійною еволюцією загроз та негативним впливом, який вони мають на приватний бізнес, державні установи та суспільство в цілому. Забезпечення високого рівня кібербезпеки вимагає адаптації існуючих методів захисту та впровадження нових стратегій, які можуть реагувати на кіберзагрози, що швидко змінюються. Крім теми впливу сучасних загроз на кібербезпеку, важливо звернути увагу на деякі важливі аспекти, які визначають ефективність підходу до протидії кібератакам.

По-перше, загрози стають більш цілеспрямованими та персоналізованими, що вимагає нових методів виявлення та реагування. Традиційних методів, заснованих на сигнатурах і правилах, часто недостатньо, оскільки кіберзлочинці все частіше використовують атаки, які оминають традиційні системи захисту. Крім технічних заходів, важливу роль відіграє і людський фактор. Зломи часто відбуваються через недостатню обізнаність користувачів про кіберзагрози або помилки, пов'язані з недотриманням кібергігієни. У цьому контексті програми навчання та підвищення обізнаності співробітників організації стали невід'ємною частиною сучасної кібербезпеки.

Удосконалення технологій штучного інтелекту та машинного навчання зробили можливим аналізувати великі обсяги даних у режимі реального часу для виявлення аномалій у поведінці мережі та системи. Ці підходи дозво-

ляють швидше реагувати на потенційні загрози та скорочують час реагування на інциденти. Хмарні обчислення також відкривають нові можливості для кібербезпеки, зокрема завдяки використанню масштабованих рішень для захисту даних і виявлення загроз. Однак це також створює нові ризики, пов'язані з централізацією даних і залежністю від хмарних провайдерів.

Висновки. Одним із перспективних напрямків залишаються архітектури нульової довіри. Він жорстко контролює доступ до ресурсів і перевірку всіх запитів, незалежно від того, надходять вони з внутрішньої чи зовнішньої мережі. Цей підхід стає все більш важливим з огляду на збільшення кількості віддалених працівників і зростання популярності гібридної інфраструктури.

Інформаційні джерела

1. Для складання тези про вплив сучасних загроз на кібербезпеку та ефективність підходів до їх 1. Stallings W., & Brown L. (2018). Computer Security: Principles and Practice. Pearson. URL: Офіційна сторінка книги на Pearson (дата звернення: 18.11.2024).

2. FireEye (2021). M-Trends 2021: Insights into Today's Cyber Attacks and Trends. FireEye Report. URL: Деталі на сайті FireEye (дата звернення: 18.11.2024).

3. NIST (2020). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, URL: Завантажити з NIST (дата звернення: 18.11.2024).

4. ISO/IEC 27001 (2013). Information technology – Security techniques – Information security management systems – Requirements. URL: Опис стандарту на офіційному сайті ISO (дата звернення: 18.11.2024).

5. Kaspersky Lab (2021). Advanced Persistent Threat (APT) Trends Report. URL: Деталі на сайті Kaspersky (дата звернення: 18.11.2024).

УДК 004.8:004.056

ЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Богдан СИРОТЕНКО
Василь ЛУЧИК
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article examines the issue of transparency and explainability of artificial intelligence (AI) systems in the context of cybersecurity and their relationship with the requirements of the EU General Data Protection Regulation (GDPR). AI transparency ensures the understandability of algorithms, which is a key factor for user trust and eliminating potential errors. The GDPR formalizes this through the obligation to explain the logic of automated decisions and the protection of personal data. The article analyzes the*

risks of algorithmic bias that can lead to discrimination, as well as the challenges of balancing cybersecurity with user privacy. It outlines the common goal of cybersecurity and GDPR regulation in ensuring ethics, transparency and reliability of systems, but highlights differences in approaches: GDPR emphasizes the protection of user rights, while cybersecurity focuses on the effectiveness of technologies to minimize threats.

Keywords: *AI transparency, GDPR, cybersecurity, explainability of algorithms, personal data protection, balance of security and privacy, discrimination, ethics of AI.*

Анотація*. У статті розглянуто питання прозорості та пояснюваності систем штучного інтелекту (ШІ) у контексті кібербезпеки та їх взаємозв'язок із вимогами Загального регламенту захисту даних ЄС (GDPR). Прозорість ШІ забезпечує зрозумілість алгоритмів, що є ключовим фактором для довіри користувачів та усунення потенційних помилок. GDPR формалізує це через обов'язок пояснення логіки автоматизованих рішень та захист персональних даних. У статті аналізуються ризики упередженості алгоритмів, що можуть призводити до дискримінації, а також виклики щодо балансу між забезпеченням кібербезпеки та збереженням приватності користувачів. Окреслено спільну мету кібербезпеки та регулювання GDPR у забезпеченні етичності, прозорості та надійності систем, але наголошено на відмінностях у підходах: GDPR акцентує увагу на захисті прав користувачів, тоді як кібербезпека фокусується на ефективності технологій для мінімізації загроз.*

Ключові слова: *прозорість ШІ, GDPR, кібербезпека, пояснюваність алгоритмів, захист персональних даних, баланс безпеки і приватності, дискримінація, етичність ШІ.*

Прозорість і пояснюваність у контексті ШІ мають на меті забезпечення можливості розуміння, як алгоритм приймає рішення. Це важливо, оскільки ШІ виконує завдання, що можуть безпосередньо впливати на безпеку користувачів та їхні системи. Зокрема, це стосується виявлення загроз, ідентифікації зловмисних дій або блокування потенційно небезпечних операцій. Непрозорі рішення можуть викликати недовіру до таких систем.

Згідно із Загальним регламентом захисту даних ЄС (GDPR), прозорість обробки персональних даних є однією з основних вимог. Регламент зобов'язує компанії пояснювати користувачам, як і з якою метою використовуються їхні дані. *Наприклад*, під час автоматизованого прийняття рішень люди мають право знати логіку цих рішень і вплив на них. Обидва підходи акцентують на пояснюваності. У кібербезпеці це має практичну функцію для усунення помилок і нарощення довіри, а GDPR націлений на забезпечення інформаційних прав користувачів. GDPR більш чітко регулює прозорість у юридичному контексті, а для ШІ це питання залишається частково технічним викликом, особливо для глибоких нейронних мереж, які часто працюють як "чорні ящики".

Ризик дискримінації виникає через використання даних, що можуть мати упередження. *Наприклад*, алгоритми можуть несправедливо виявляти активність певних груп користувачів як підозрілу, базуючись на історич-

них даних або географічних особливостях. Таке упередження може впливати на доступ до ресурсів або блокування дій, що насправді є безпечними. Регламент прямо забороняє дискримінацію через автоматизовану обробку даних. *Наприклад*, обробка персональних даних не повинна призводити до несправедливих результатів або дискримінації через расову, етнічну чи соціальну належність, гендер або інші особисті ознаки. GDPR також заохочує впровадження незалежного моніторингу алгоритмів. І GDPR, і етичний підхід до ШІ в кібербезпеці передбачають уникнення дискримінації як важливу мету. Вони наголошують на необхідності регулярного аудиту моделей, щоб запобігти упередженості. GDPR зосереджений на захисті прав людини, тоді як у кібербезпеці акцент робиться на забезпеченні коректної роботи алгоритмів у реальних умовах.

ШІ може покращити кібербезпеку, *наприклад*, через моніторинг трафіку або аналіз поведінкових патернів. Однак це часто потребує збору великого обсягу даних, які можуть містити конфіденційну інформацію. Відсутність балансу між безпекою та приватністю може призвести до надмірного втручання в особисте життя користувачів. Регламент встановлює суворі правила для обробки персональних даних, зокрема вимогу мінімізувати обсяг зібраної інформації та використовувати її лише для чітко визначених цілей. Це включає зобов'язання компаній захищати приватність користувачів і гарантувати, що дані не використовуються поза межами заявлених цілей.

Обидві сфери визнають важливість балансу ШІ в кібербезпеці спрямований на обмеження доступу до надмірних даних, тоді як GDPR формалізує це правило. GDPR ставить права користувача на перше місце, навіть якщо це може ускладнити роботу кібербезпекових систем. Водночас, у кібербезпеці часто робиться акцент на пріоритеті безпеки, навіть якщо це частково обмежує приватність.

Висновки. GDPR і використання ШІ в кібербезпеці мають спільну мету – забезпечення надійності та етичності роботи систем, однак вони мають різні підходи. GDPR формалізує прозорість і захист прав, а кібербезпека прагне балансувати між ефективністю технологій і мінімізацією ризиків для користувачів.

Інформаційні джерела

1. Регламент Європейського парламенту і Ради (ЄС). URL: https://zakon.rada.gov.ua/go/984_008-16 (дата звернення: 21.11.2024).

2. Посібник з європейського права у сфері захисту персональних даних. URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf (дата звернення: 19.11.2024).

3. Загальний регламент про захист даних Європейського Союзу. URL: https://www.esri.com/uk-ua/privacy/privacy-gdpr (дата звернення: 20.11.2024).

УДК 621.392

АПАРАТИ ЗАХИСТУ В СИСТЕМАХ SMART HOUSE

Володимир ШВЕДОВ
Юрій РУДИК
Львівський державний університет безпеки життєдіяльності
м. Львів, Україна.

Abstract. *One of the warehouse "smart booths" includes electrical protection devices, which ensure the control system's safety, including the Building Management System. The devices protect against emergency situations, against short circuits, threats of fire and overvoltages (as protection against impulse overvoltages). Integration of SPD with BMS allows you to increase reliability significantly, and automated monitoring allows you to identify problems at early stages.*
Keywords: *Smart houses, electrical protection devices, control systems, BMS, SPD, fire safety.*

Анотація. *Однією з складових "розумних будинків" є апарати електричного захисту, які відповідають за безпеку системи управління, у тому числі Building Management System. Апарати захисту запобігають аварійним ситуаціям, зокрема коротким замиканням, загрозам загоряння та перенапругам (як захист від імпульсних перенапруг). Інтеграція SPD у BMS дозволяє значно підвищити надійність, оскільки автоматизований моніторинг дає змогу виявляти проблеми на ранніх етапах.*
Ключові слова: *Розумні будинки, апарати електричного захисту, системи управління, перенапруги, пожежна безпека.*

Інтелектуальні системи управління житлом, відомі як Smart House, набувають все більшої популярності завдяки можливості автоматизувати контроль за електрообладнанням і забезпечити високий рівень комфорту та безпеки.

Аналіз публікацій [1] свідчить, що напрям розвитку систем електропостачання це інфраструктури: p2p-ринку для домогосподарств, мереж зарядок електромобілів, сервіси demand response. Це призведе до подальшого збільшення вимог до точності, безпеки та захисту електропостачання, зокрема збільшення вимог до апаратів захисту.

За [2], ринок електроенергії змінюється завдяки зростаючій інтеграції розподілених енергетичних ресурсів, а також необхідності забезпечення підвищення надійності, стійкості та ефективності мереж передачі та розподілу електроенергії, відповідно, можна усвідомити, що сучасне обладнання є чутливим до імпульсних перенапруг, які виникають в мережі, а також при ударі блискавки. Як наслідок, підвищення надійності апаратів захисту у системі пожежної безпеки відіграє важливу роль в розвитку сучасних електроінсталяцій.

Однією з ключових складових систем безпеки "розумних будинків" є апарати електричного захисту, які відповідають за безпеку системи керування,

а також запобігають аварійним ситуаціям, зокрема коротким замиканням, перенапругам та загрозам загоряння. Building Management System (BMS) є комплексною системою управління інженерними мережами будівлі, що забезпечує автоматизацію процесів контролю та управління такими підсистемами, як освітлення, опалення, вентиляція, кондиціювання, системи безпеки та енергоспоживання. Одним із критично важливих аспектів надійного функціонування BMS є захист електромережі від перенапруг, які можуть виникати через грозові розряди, стрибки напруги або комутаційні процеси.

До основних типів апаратів електричного захисту належать запобіжники, автоматичні вимикачі, диференційні автомати, обмежувачі перенапруг (ОПН), пристрої захисту від імпульсних перенапруг (SPD), ізоляційні монітори та реле напруги. Їх інтеграція в систему "розумного будинку" забезпечує як фізичний захист електроустановок, так і автоматизований контроль за їх станом.

Електричні перенапруги є короткочасними підвищеннями напруги в мережі, що можуть мати як природний, так і техногенний характер. Основні причини включають:

– атмосферні перенапруги: викликані блискавками;

– комутаційні перенапруги: спричинені вмиканням або вимиканням потужного обладнання;

– індуктивні перенапруги: спричинені взаємодією ліній живлення з іншими електромагнітними полями.

Наслідки перенапруг можуть включати пошкодження або вихід з ладу електронного обладнання, збої в роботі систем BMS, зниження терміну служби компонентів та підвищення ризику загоряння.

Обмежувачі перенапруг (ОПН) (SPD – Surge Protective Devices) визначаються базовим складником [3] внутрішнього блискавкозахисту, а також нормативних вимог до захисту від перенапруги, що підкреслює актуальність дослідження їх впливу на пожежну безпеку.

Особливо актуальними є ОПН, які захищають електромережі від імпульсних перенапруг, що виникають під час грозової активності або різких стрибків напруги в мережі. Згідно з нормами ПУЕ, для ефективного захисту електроустановок до 3 кВ необхідно забезпечити опір розрядників не менше 1000 МОм. У випадку повітряних ліній живлення із значною грозовою активністю (понад 25 годин на рік) застосовуються засоби категорії II захисту.

В цій статті [4] вказано, що особливо небезпечною є система TN-C-S вказана в ПУЕ для сільських побутових електроспоживачів з повітряними живильними лініями 380/220 В, оскільки сільські ПЛ-0,38 кВ відрізняються своєю великою довжиною і розгалуженістю. При обриві PEN-провідника (що в сільських електромережах, при їхній великій розгалуженості, має високу імовірність) на всіх металевих корпусах електроприймачів, приєднаних до захисного PE-провідника (тобто включених в євророзетки), з'являється смертельно небезпечний потенціал фази.

Залежно від застосування SPD поділяються на захист ліній живлення (L), сигнальних ліній (S) та комбінований захист (C).

Інтеграція SPD у BMS дозволяє значно підвищити надійність всієї системи, оскільки автоматизований моніторинг та діагностика стану захисних пристроїв дають змогу виявляти потенційні проблеми ще на ранніх етапах. *Наприклад*, у разі виявлення підвищеного рівня перенапруги система може автоматично вивести з експлуатації небезпечні ділянки мережі, мінімізуючи ризики пошкоджень.

Ефективне функціонування апаратів захисту в системі "розумного будинку" неможливе без регулярного тестування та діагностики. Одним із перспективних методів є імітаційне моделювання, яке дозволяє відтворювати різні сценарії аварійних ситуацій та оцінювати роботу захисних пристроїв. *Наприклад*, для пристроїв класу I використовується імпульс струму з формою хвилі 10/350 мкс для симуляції прямого удару блискавки, що дає змогу перевірити їх надійність у критичних умовах.

В [5] вказаноно, що при випробувані SPD використовують іскрові проміжки між лініями живлення і землею зі значною здатністю гасити струм що робить їх застосовними в електромережах з перспективою витримування струму короткого замикання в десятки кА.

Сучасні тенденції в розвитку Smart House передбачають впровадження інтелектуальних систем захисту, які здатні не лише реагувати на надзвичайні ситуації, а й прогнозувати їх. Завдяки використанню алгоритмів аналізу даних та штучного інтелекту такі системи можуть визначати потенційні загрози, автоматично приймати рішення про відключення або переналаштування мережі, що мінімізує ризик аварійних ситуацій. Інтеграція підвищеної надійності апаратів електричного захисту в систему таких будинків значно підвищує рівень безпеки користувачів та обладнання. Завдяки постійному моніторингу, аналізу даних та автоматизованому управлінню система може своєчасно виявляти та усувати потенційні загрози. Подальший розвиток технологій штучного інтелекту та аналітики даних сприятиме створенню ще більш надійних та адаптивних систем захисту.

Захист від електричних перенапруг є важливою складовою надійного функціонування системи Building Management System. Розвиток сучасних SPD дозволяє не лише забезпечити захист обладнання, а й підвищити загальну надійність та безпеку інфраструктури. Подальший розвиток інтелектуальних технологій у цій галузі сприятиме створенню більш гнучких і надійних систем управління будівлями.

Висновки. Отже, апарати електричного захисту є невід'ємною частиною сучасних систем Smart House. Вони забезпечують надійність, пожежну безпеку та ефективність електричних мереж завдяки автоматизації процесів моніторингу, діагностики та захисту. Підвищення надійності апаратів захисту у "розумних будинках" та інтеграція інтелектуальних рішень у цю сферу є важливим кроком на шляху до підвищення рівня комфорту та безпеки.

Інформаційні джерела

1. Rudyk Yu., Nazarovets O., Golovatchuk I. Current approaches in the system lightning protection arrangement of buildings in view of fire hazard and personal risk, Fire Safety, Lviv State University of Life Safety, 2019. URL: https://doi.org/10.32447/20786662. 33.2018.12

2. Campos do Prado J., Qiao W., Qu L., Aguero J. (2019). The Next-Generation Retail Electricity Market in the Context of Distributed Energy Resources: Vision and Integrating Framework. URL: https://www.researchgate.net/publication/330890414_The_nextgeneration_Retail_Electricity_Market_in_the_Context_of_Distributed_Energy_Resources_Vision_and_Integrating _Framework

3. Faria da Silva F., Pedersen K (2022). Lightning surges in hybrid cable-overhead lines: Part I–voltage estimation for shielding failure. Electr Eng 104, pp. 3281–3294. URL: https://doi.org/10.1007/s00202-022-01538-z

4. Rudyk Yuriy, Kuts Victor, Nazarovets Oleg, Zdeb Volodymyr. Complex Tools for Surge Process Analysis and Hardware Disturbance Protection, Data-Centric Business and Applications, Springer International Publishing, 2021. URL: https://link.springer.com/chapter/ 10.1007/978-3-030-71892-3_9

5. Волощук Л. О. Економічна безпека та інноваційний розвиток промислового підприємства: сутність та взаємозв'язок як об'єктів управління ЕКОНОМІКА: реалії часу ECONOMICS: time realities №6(16), 2014. URL: http://dspace.opu.ua/jspui/bitstream/ 123456789/1821/1/217-223.pdf.

УДК 004.4

СИСТЕМА ОХОРОННОЇ СИГНАЛІЗАЦІЇ НА ОСНОВІ ПЛАТФОРМИ ARDUINO

Максим КУТНЯК
Леонід КУПЕРШТЕЙН

Вінницький національний технічний університет м. Вінниця. Україна.

Abstract. *The work is devoted to the improvement of the security alarm system based on the Arduino platform. A scientific research and feasibility study of the research has been prepared. The work analyzes existing security alarm systems and justifies the choice of the platform for implementation. Keywords: Arduino, sensor, reed switch, PIR, buzzer, GSM, SIM, SMS, display, microclimate, temperature, relative humidity.*

Keywords: *alarm, Arduino, sensor, reed switch, PIR, GSM, SIM, SMS, display.*

Анотація. *Робота присвячена вдосконаленню системи охоронної сигналізації. Підготовлено науково-дослідне та техніко-економічне обґрунтування доцільності досліджень. У роботі здійснено аналіз існуючих систем охоронних сигналізації і обґрунтовано вибір платформи для реалізації.Ключові слова: Arduino, датчик, геркон, PIR, бузер, GSM, SIM, SMS, дисплей, мікроклімат, температура, відносна вологість.*

Ключові слова: *сигналізація, Arduino, датчик, геркон, PIR, GSM, SIM, SMS, дисплей.*

Сьогодні цифровізація життя сприяє перенесенню все більшої кількості даних в електронну форму, що впливає на різні сфери діяльності, включаючи системи безпеки та охорони. З розвитком технологій охоронні системи стають все більш інтелектуальними та здатні обробляти велику кількість інформації в режимі реального часу. Програмне забезпечення, яке використовується в таких системах, виконує роль основної ланки для обробки даних різного рівня важливості, що підвищує вимоги до забезпечення їх захищеності [1].

При створенні системи охоронної сигналізації на основі платформи Arduino важливо гарантувати фізичну безпеку. До таких даних відносяться сигнали від датчиків, керуючі команди та внутрішня інформація системи, яка формується, зберігається та використовується під час роботи.

Актуальність. Забезпечення безпеки людей та майна завжди було й залишається одним з найважливіших завдань суспільства. Охоронні сигналізації (ОПС) відіграють ключову роль у попередженні пожеж, незаконного проникнення та інших надзвичайних ситуацій. Традиційні ОПС, як правило, ґрунтуються на дорогих та складних компонентах, що робить їх доступними не для всіх. Цей недолік робить актуальним пошук альтернативних рішень, які б поєднували в собі ефективність, доступність та простоту використання [2].

Мікроконтролери Arduino пропонують себе як перспективну платформу для розробки ОПС нового покоління. Завдяки своїй доступності, простоті програмування та гнучкості, Arduino робить можливим створення надійних та економічних систем сигналізації, які можуть бути адаптовані до різноманітних потреб [3].

Однією з таких критичних областей застосування кібербезпеки є проектування систем безпеки, зокрема охоронно-пожежних сигналізацій. Зростаюча складність сучасних будівель, споруд та інфраструктурних об’єктів вимагає вдосконалення систем безпеки, що забезпечує реагування на небезпеку в реальному часі та надійний захист користувачів. Водночас, зростаюча кількість пожежних та кібератак на інфраструктуру додає складності до цієї проблеми [4].

Проектування охоронно-пожежних систем на базі мікроконтролерів Arduino представляє собою перспективний шлях для забезпечення ефективного контролю та реагування на потенційні загрози. Arduino, як відомий відкритий апаратний та програмний засіб, дозволяє розробникам створювати кастомізовані рішення з високим рівнем гнучкості та доступності. Його використання в охоронно-пожежних системах дозволяє створювати інтегровані, ефективні та стійкі до кібератак рішення [5].

Переваги системи на основі Arduino. Гнучкість та адаптивність, можливість легко змінювати конфігурацію системи під конкретні потреби користувача завдяки відкритому програмному забезпеченню. Доступність, відносно невисока вартість компонентів та простота збирання дозволяють створити систему за доступною ціною. Розширюваність, можливість підключення додаткових датчиків та модулів для розширення функціоналу системи.

Енергоефективність, Arduino відрізняються низьким споживанням енергії, що дозволяє використовувати систему в автономному режимі [6].

Потенційні сфери застосування. Житлові приміщення, захист квартир, будинків від проникнення, пожежі, витоку газу. Офіси та підприємства, контроль доступу, моніторинг стану приміщень, сповіщення про нештатні ситуації. Сільське господарство, контроль температури та вологості в теплицях, моніторинг стану тварин [7].

З огляду на переваги та потенційні сфери застосування, розробка системи охоронної сигналізації на основі платформи Arduino є цілком доцільною.

На рисунку1 представлена монтажна схема системи охоронної сигналізації на основі платформи Arduino.

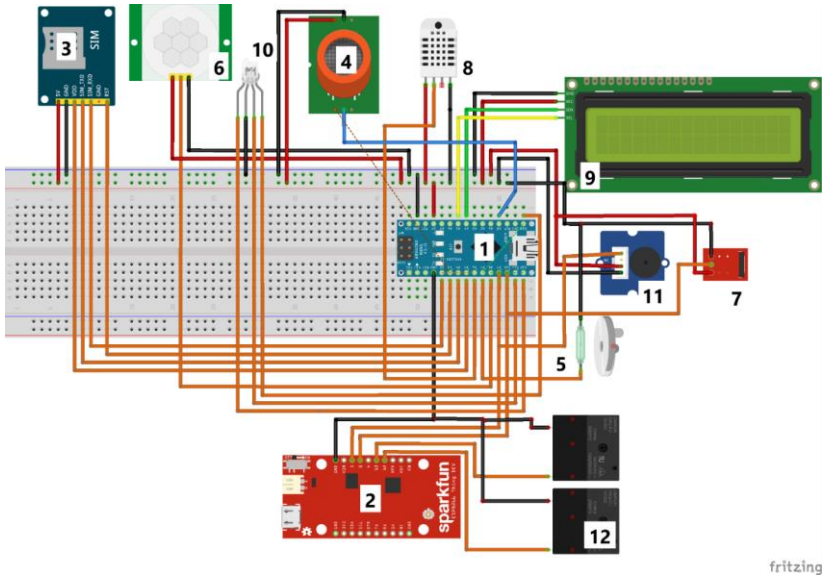


Рисунок 1 − Монтажна схема системи охоронної сигналізації на основі платформи Arduino

Принцип роботи системи. Датчик відчинення дверей та датчик руху передають інформацію до мікроконтролера, мікроконтролер спілкується з GSM модулем для обміну інформації по SIM. Датчики температури, вологості та якості повітря передають значення відповідних фізичних величин на мікроконтролер. Символьний дисплей та світлодіод слугує для інформування користувача про стан системи та потрібною інформацією. Для прикладу, на дисплей виводиться значення температури в градусах Цельсія, яке передали датчики мікроклімату. ESP8266 з'єднане з головним мікроконтролером

по UART, ESP8266 має на собі WiFi модуль, який під'єднується до наявної точки доступу, через мережу інтернет з'єднується з сервером, який у свою чергу, з'єднує мобільний додаток та систему.

Висновки. Згідно з дослідженнями було розглянуто та обґрунтовано доцільність використання платформи Arduino для проектування сучасних охоронних систем. Запропонована система інтегрує різноманітні датчики для моніторингу як безпеки, так і мікроклімату приміщення, забезпечуючи багаторівневий контроль. Інноваційним є використання GSM модуля для сповіщення та модуля ESP8266 для віддаленого управління, що дозволяє оперативно реагувати на загрози. Це робить розроблену систему ефективним та надійним інструментом для захисту майна і життя користувачів, відкриваючи перспективи для її подальшого розвитку та адаптації.

Інформаційні джерела

1. Цифровізація. URL: https://razumkov.org.ua/statti/ tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyklykiv

2. Системи охоронної сигналізації. URL: https://alarm. lviv.ua/systemy-bezpeky/syhnalizatsiia/systemy-okhoronnoi-syhnalizatsii

3. Arduino. URL: https://uk.wikipedia.org/wiki/Arduino

4. Стратегічний аналіз безпекового середовища України. URL: https://niss.gov.ua/news/statti/stratehichnyy-analiz-bezpekovoho-seredovyshcha-ukrayin

5. Охоронна сигналізація. URL: https://ukrinfosystems. com.ua/uk/design-and-construction/alarm-system

6. Архітектура технології Arduino та її переваги. URL: https://uk.fmuser.net/content/?10729.html

7. Сигналізація для дому. URL: https://imperia.org.ua/ article/signalizaciya-dlya-domu-vse-scho-potribno-znati-pro-ohoronnu-signalizaciyu-dlya-budinku

Напрям 8

ІНФОРМАЦІЙНІ ВІЙНИ

УДК 004.056.5

ФЕЙКОВІ НОВИНИ ЯК ІНСТРУМЕНТ СУЧАСНОГО ПРОТИСТОЯННЯ

Ростислав КІСІЛЬ
Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The thesis examines the phenomenon of fake news as a tool of modern information warfare. The main characteristics of fake information, its impact on society, in particular social polarization, loss of trust in the media, provoking panic and threat to democratic processes are considered. The main reasons for the popularity of fake news are highlighted, such as the use of social networks, economic benefit and political manipulation. Also analyzed are possible ways of combating disinformation, in particular through education, fact-checking, technologies and legal mechanisms. The need for a responsible attitude to the consumption of information and the development of critical thinking is emphasized.*

Keywords: *fake news, disinformation, information war, social networks, manipulation, media literacy, fact-checking, critical thinking, threat to democracy.*

Анотація. *У тезі досліджено феномен фейкових новин як інструменту сучасної інформаційної війни. Розглянуто основні характеристики фейкової інформації, її вплив на суспільство, зокрема соціальну поляризацію, втрату довіри до медіа, провокування паніки та загрозу демократичним процесам. Виділено основні причини популярності фейкових новин, такі як використання соціальних мереж, економічна вигода та політичні маніпуляції. Також проаналізовано можливі шляхи боротьби з дезінформацією, зокрема через освіту, фактчекінг, технології та правові механізми. Наголошено на необхідності відповідального ставлення до споживання інформації й розвитку критичного мислення.*

Ключові слова: *фейкові новини, дезінформація, інформаційна війна, соціальні мережі, маніпуляція, медіаграмотність, фактчекінг, критичне мислення, загроза демократії.*

Вступ. На початку варто зазначити, що інформація в сучасному світі є потужною силою, яка може перевершувати навіть традиційні види 21 століття. У суспільстві, де доступ до Інтернету має більшість населення, фейкові новини стали засобом масового впливу, здатним змінювати політичний курс, викликати соціальні заворушення та впливати на міжнародні відносини.

Основна частина. Хоча термін “фейкові новини” набув популярності лише в останнє десятиліття, саме явище має давнє коріння. Ще за середньовіччя неправдиві чутки використовувалися для ослаблення супротивників, а під час Холодної війни дезінформація стала звичним інструментом глобального протистояння. В наші дні цифрових технологій масштаби і швидкість поширення фейкової інформації досягли небаченого рівня. Ця робота має на меті проаналізувати фейкові новини як інструмент сучасної інформаційної війни, досліджуючи їх вплив на суспільство та виявляючи ефективні методи боротьби з ними.

1. Сутність та характеристики фейкових новин Фейкові новини створюються навмисно з метою маніпулювання або досягнення певних цілей через неправдиву інформацію. Основні особливості фейків:

– Швидке поширення. Завдяки соціальним мережам і месенджерам фейки можуть досягати мільйонів людей за лічені години.

– Маніпулювання емоціями. Вони часто призначені для того, щоб викликати страх, гнів або співчуття та впливати на поведінку аудиторії.

– Реалістичний вигляд. Фейкові новини часто імітують дизайн авторитетних ЗМІ, маскуючися під реальні джерела. *Наприклад*, у 2020 році під час пандемії COVID-19 широко поширювалися фейки про “чіпування вакцин”, що спричинило глобальну недовіру до системи охорони здоров’я.

2. Причини популярності фейкових новин Фейкові новини користуються популярністю через декілька чинників:

– Соціальні мережі як платформа. Facebook, Twitter і TikTok сприяють їх швидкому поширенню без повного контролю над правдивістю.

– Економічна вигода. Багато з них створюються для залучення трафіку і заробітку на рекламі.

– Політичні цілі. Уряди або групи використовують фейки для дискредитації опонентів, зміни громадської думки або посіву паніки [1].

– Відсутність критичного мислення у громадян, які часто не перевіряють інформацію і приймають її за чисту монету.

Ці фактори створюють ідеальні умови для поширення дезінформації в сучасному суспільстві [2].

3. Використання фейкових новин у глобальних протистояннях.

Фейкові новини стали значущою частиною сучасної інформаційної війни між країнами. Вони можуть використовуватися для:

– Політичного впливу. *Наприклад*, у 2016 році під час виборів у США російські агентства поширювали неправдиві матеріали для дискредитації одного з кандидатів.

– Військової пропаганди. Під час конфлікту в Україні активно поширювалися фейки про дії української армії, що спрямовані на зниження морального духу суспільства та міжнародну ізоляцію країни.

– Культурного впливу. Створення негативного образу певної культури або країни через фейки. Фейкові новини є частиною "гібридної війни", яка поєднує фізичні та інформаційні методи боротьби.

4. Наслідки поширення фейкових новин. Розповсюдження хибної інформації може призвести до серйозних наслідків:

– Соціальна поляризація. Фейкові новини посилюють розбіжності в суспільстві та провокують конфлікти між різними групами людей. Паніка. *Наприклад*, у 2022 році через чутки про "радіаційний вибух" в Україні відбулася масова закупівля йоду. Втрата довіри до медіа. Люди починають сумніватися в усій інформації, включно з правдивою.

– Загроза демократії. Фейки можуть впливати на результати виборів, підриваючи демократичні процеси [3].

5. Як боротися з фейковими новинами? Ефективна боротьба з фейковими новинами потребує системного підходу:

– Освітні програми. Підвищення медіаграмотності та розвиток критичного мислення у суспільстві.

– Фактчекінг. Платформи на кшталт StopFake активно перевіряють і спростовують неправдиву інформацію.

– Технології. Використання штучного інтелекту для ідентифікації дезінформації. Правові засоби. Підвищення відповідальності за свідоме поширення фейкових новин.

Також незалежні журналісти грають ключову роль у гарантуванні об'єктивності та прозорості.

Висновки. Фейкові новини є одним з найбільших викликів у сучасному інформаційному середовищі. Вони можуть дестабілізувати суспільство, впливати на політику і підривати довіру до ЗМІ. Однак завдяки освіті, технологіям і співпраці на глобальному рівні їх вплив можна значно зменшити.

Кожен з нас несе відповідальність за ту інформацію, яку ми споживаємо і розповсюджуємо. Розвиток критичного мислення та уважне ставлення до джерел є важливими інструментами у боротьбі з фейковими новинами в умовах сучасних викликів.

Інформаційні джерела

1. Detector.media. Дезінформація, пропаганда і все, що між ними: як розпізнати і захиститися. detector.media. URL: https://detector.media/withoutsection/article/201754/2022-08-10-dezinformatsiya-propaganda-i-vse-shcho-mizh-nymy-yak-rozpiznaty-i-zakhystytysya/ (дата звернення: 18.11.2024).

2. Лотоцька Н. Україна найчастіше є жертвою дезінформації та фейків, − звіт Європейської служби зовнішніх справ. LB.ua. URL: https://lb.ua/society/2024/01/25/595364_ukraina_naychastishe_ie_zhertvoyu.html (дата звернення: 18.11.2024).

3. Тюхтенко Є. Які основні меседжі прокремлівської пропаганди? Шість країн презентували свої дослідження. *Радіо Свобода*. URL: https://www.radiosvoboda.org/a/28339105.html (дата звернення: 18.11.2024).

УДК 004.9:659.1

ФІШИНГ ЯК ЗАГРОЗА ОНЛАЙН СЕРЕДОВИЩА

***Володимир САБАТ*[1]**
***Віталій МАЦЮК*[2]**
[1]Інститут поліграфії та медійних технологій Національного університету "Львівська Політехніка", м. Львів, Україна.
[2]Відокремлений структурний підрозділ "Львівський поліграфічний фаховий коледж Української академії друкарств", м. Львів, Україна.

Abstract. *The concept of "phishing" is considered. The main types of phishing attacks are highlighted. Channels of distribution, ways and methods of phishing attacks are analyzed. Practical recommendations are given on how to protect personal data from the harmful effects of phishing messages and information threats spread over the Internet.*
Keywords: *phishing, information threat, data protection, countering phishing attacks.*

Анотація. *Розглянуто поняття "фішингу". Виокремленні основні види фішингових атак. Проаналізовано канали поширення, способи і методи здійснення фішингових атак. Надано практичні рекомендації щодо захисту персональних даних від шкідливого впливу фішингових повідомлень та інформаційних загроз що поширюються через мережу Інтернет.*
Ключові слова: *фішинг, інформаційна загроза, захист данних, протидія фішинговим атакам.*

Сьогодні, у час неоголошеної війни країни-агресора росії проти України і посиленого зростання кібератак на об'єкти критичної інфраструктури, ворог використовує витончені атаки психологічного впливу на людей, за допомогою мережі Інтерент, електронної пошти, поширенням спаму та негативної інформації через соціальні мережі. Одним із наймасових методів пропаганди та дезінформації від зловмисників вважається використання реклами та актуальних для користувача-жертви повідомлень, за якими він стежить і відкриває на своєму персональному комп'ютері (ПК). Такі повідомлення, що містять в собі посилання на відкриття тієї чи іншої інформації у вигляді файлів чи покликань відвідати певні веб-ресурси на перший погляд не можуть містити в собі ніякої загрозливої для користувача інформації, бо видаються замаскованими під популярні в мережі сайти. Але насправді, за допомогою таких атак, спрямованих на залучення уваги користувача, здійснюється викрадання їхньої персональної інформації з метою подальшої дезоргнаізації, шантажу та поширення спаму через отримані ресурси з інформацією про друзів-корисувача. Таким чином відбуваються фішингові атаки, які замасковані під позитивний для користувачів мережі Інтернет контент. Фішинг (від англ. *fishing – риболовля*) – це одна з найпоширеніших загроз у

кіберпросторі, що дозволяє зловмисникам викрадати персональні дані користувачів, клієнтів та будь яких інших соціальних агентів, що в тій чи інші мірі користуються мережею Інтернет.

У звіті Phishlabs про тенденції в області фішингу, ще перед повномасштабним вторгненням росії в Україну, за третій квартал 2021 року [1] вказується, що фішингові атаки зрісли майже на 32% у порівнянні з попереднім роком, голосові фішингові дзвінки та пов'язані з цим інциденти зросли більш ніж вдвічі, фішингові загрози з соціальних мереж зросли на 82%, при цьому кількість фішингових повідомлень щоразу збільшується, зловмисники використовують різні напрямки атак: електронну пошту, соціальні мережі, мобільні пристрої та інші. У них також є доступ до безкоштовних SSL-сертифікатів. Більша половина усіх фішингових веб-сайтів використовує протокол HTTPS, який був одним з основних індикаторів легітимності веб-сайтів [2].

Згідно з вітчизняною статистикою за період з 01.01.2021 по 01.07.2021 – 6 тис. опитаних осіб (із 55 тис. респондентів) отримували фішингове посилання від шахраїв. З них – 18% українців, які стикалися із шахрайством у 2021 році, не знають жодного способу захисту своїх платіжних даних, про методи протидії шахрайству – 51% опитаних дізналися із соцмереж, 31% – від друзів, 18% – з телебачення. Майже 40% українців уже знають, що надіслані посилання від малознайомих людей можуть бути шахрайською такою, тому не відкривають їх і не обговорюють фінансові питання в месенджерах, якщо співрозмовник поводиться підозріло. 20% перевіряє користувача за номером телефону, 14% – уважно вчитується в зміст сторонніх SMS та електронних листів, а 10% – перевіряє посилання сайтів, щоб не потрапити на фішинговий сайт [3, 4].

Найбільш поширеними видами фішингових атак є:

1. Фішинг веб сайтів. Цей спосіб характеризується тим, що злочинці створюють підроблені (фейкові) веб-сайти. На зовнішній вигляд інтерфейс цих сайтів може нічим не відрізнятись від справжніх. Зазвичай це сайти банків, соціальних мереж, Інтернет-магазинів тощо, де зловмисники просять користувачів ввести свої дані для "санкціонованого" входу. Це виглядає таким чином: користувач отримує посилання на фейковий сайт, вводить там свої конфіденційні дані для входу і вони потрапляють до рук зловмисників. Дуже часто в таких сайтах використовуються скорочені посилання (*наприклад*, goo., bit., gl.) щоб залучити довіру до них користувача і якнайкраще приховати їхню фішингову сітність.

До практичних рекомендацій боротьби з фішінгом та протидією таким загрозам є уникання переходів за підозрілими посиланнями і ретельна перевірка URL-адрес усіх сайтів на які відбуваються посилання. Також, дуже часто довгі посилання для переходів можуть бути небезпечними. Особливу увагу потрібно звертати на доменне ім'я та підозрілі символи в лінках. Краще самостійно, вручну вводити адреси електронних сервісів у браузері. Також

якщо виникають підозри у достовірності веб-ресурсу – можна скористатись пошуковою системою для перевірки його автентичності.

2. Фішинг в електронній пошті. Фішингові листи пропонують користувачеві перейти за посиланням або відкрити долучені до цього листа файли, які скоріш за все містять шкідливий програмний код або можуть перенаправляти його на фішингові сайти. У цьому випадку фішингова атака розвивається таким чином: користувач отримує електронний лист від нібито знайомого сервісу або особи з проханням оновити інформацію, підтвердити проведення списання коштів (транзакції) тощо. А подальші дії зловмисників як і в п. 1 – отримання конфіденційних даних від користувача.

3. Фішинг в соціальних мережах та месенджерах. Соціальні мережі використовуються зловмисниками для розсилання повідомлень з підозрілими посиланнями. Один із варіантів вмісту підозрілих повідомлень в соціальних мережах і месенджерах, поширених сьогодні, – прохання надати особисту інформацію. Алгоритм таких дій наступний: користувач отримує повідомлення від "члена сім'ї", "друга" чи "знайомої людини" з прохання про допомогу з посиланням на актуальну новину. *Наприклад*, це можуть бути повідомлення щодо фінансової допомоги при травмуванні, втраті майна, допомозі збройним силам України тощо. Розпізнати фішинг в таких повідомленнях для користувачів соціальних мереж стає дедалі складнішим способом. Основним фактором, що спонукає користувачів виконувати сценарії фішингових атак є те, що такі повідомлення зазвичай приходять він нібито знайомих людей, до яких у користувача вже є довіра. Також зловмисники збирають інформацію про уподобання користувачів, використовують бездоганну мову та іноді маскуються під відомих усім людей.

Методи протидії такого роду повідомленням зводяться до перевірки створення повідомлень від відправників до їхнього змісту. Зазвичай у таких випадках достатня двохфакторна автентифікація істинності повідомлення, за допомогою телефонного дзвінка до його відправника. Але, навіть якщо щось видається підозрілим, краще такі повідомлення ігнорувати.

Також фішингові сайти, створенні зловмисником, можуть пропонувати підписатись на календар, видаючи це за необхідність, що покращить роботу чи користування ними користувачеві. Проте тут може бути прихована загроза. Підписавшись на такий календар, користувачеві можуть почати надходити регулярні сповіщення, що виглядатимуть як системні, але міститимуть посилання на фішингові сайти. Схожа ситуація і з сповіщеннями. Якщо користувач дає згоду на їх отримання, дуже ймовірно що з певною періодичністю він буде отримувати повідомлення з посиланням на фішингові ресурси. Щоб убезпечити себе від таких загроз необхідно завжди перевіряти від кого саме надходять такі сповіщення. Якщо такі повідомлення надходять від незнайомих людей, або виглядають підозріло, тоді краще взагалі не відкривати такі повідомлення. Також

користувач може перевірити значущість таких повідомлень, давши відповідь на такі питиання: “Чи очікував я на це повідомлення? ”, “Чому мені надіслали це посилання? ”, “Чи знаю я цього відправника? ”.

Фішинг не обмежується лише текстовими повідомленнями. Шахраї також можуть використовувати і телефонні дзвінки, в яких можуть видавати себе за кого завгодно. *Наприклад*, за співробітника банку. В допомогу, при виконанні шахрайських дій, злочинці використовують штучний інтелект. Завдяки йому, шахраї можуть імітувати голос і навіть зовнішність, у випадку відеодзвінків. Для перевірки таких повідомлень необхідно також зв’язатись з особою альтернативними каналами зв’язку.

Особливу увагу необхідно звернути на збільшення фішингових атак на ієрархічні системи управління критичною інфраструктурою, що дуже актуально сьогодні, коли ворог використовує будь-які методи дестабілізації нашої економіки для примусу нас до швидкої капітуляції. В цьому випадку такі атаки здійснюються через осіб, які здатні приймати рішення в кризових ситуаціях, тому дуже важливо також вчасно інформувати усіх причетних до виробничого процесу про методи здійснення фішингових атак та їхню небезпеку. Так, *наприклад*, якщо фішинг зловмисниками здійснюється на приватних осіб з метиою заволодіння їхнім акаунтом в соціальних мережах чи банківськими реквізитами для наживи, то такі дії на осіб, що приймають рішення в ієрархічній системі з управління об’єктами критичої інфораструктури, можуть призвести до аварійних ситуацій і виведення іх з ладу, що вкрай небезпечно в наших умовах [5].

Висновки. Фішинг – це серйозна загроза для користувачів онлайн. Щоб правильно захистити себе, необхідно знати його види, щоб мати змогу розпізнавати ознаки шахрайства. Також в нагоді стане використання критичного мислення. Перевірка посилань на джерела інформації, використання альтернативних каналів зв’язку для підтвердження підозрілих запитів убезпечить користувачів від фішингових атак. Дотримання таких порад захистить користувачів від загроз та забезпечить захист даних.

Інформаційні джерела

1. Quarterly threat trends & intelligence report November 2021. URL: https:// info.phishlabs.com/hubfs/PhishLabs%20-%20QTTI%20Report%20-%20 November% 202021.pdf.

2. Patrick Nohe. HTTPS Phishing: 49% of Phishing Websites Now Sport The Green Padlock. URL: https://www.thesslstore.com/blog/https-phishing-green-padlock/

3. Українці почали вдвічі частіше стикатися з шахраями в інтернеті, найбільше – в месенджерах: результати опитування. URL: https://blog.olx.ua/ 26779/ ukra%d1%97nci-stali-vdvichi-chastishe-stikatisya-z-shaxrayami-v-interneti-najbilshe-vmesendzherax-rezultati-opituvannya/#

4. Думчиков С. А., Лукічов В. В. Статистика фішингових інцидентів в Україні за 2021 рік. Вінницький національний технічний університет. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34523/91970.pdf?sequence=2&isAllowed=y

5. Сікора Л. С., Лиса Н. К., Сабат В. І., Мацюк В. В. Антикризове управління соціальними об'єктами за допомогою інформаційних рекламних повідомлень в умовах загроз / Науковий вісник НЛТУ України, Національний лісотехнічний університет України, 2024. № 4. – С. 49–58. URL: https://doi.org/10.36930/40340407.

УДК 355.357:004.9

РОЗУМІННЯ МАЙБУТНІМИ ОФІЦЕРАМИ ЗНАЧУЩОСТІ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ У ПРОЦЕСІ ЦИВІЛЬНО-ВІЙСЬКОВОЇ ВЗАЄМОДІЇ

Наталія СНАПКОВА
Державний український університет імені Михайла Драгоманова, м. Київ, Україна.

Abstract*. Defining information warfare as a multifaceted and complex phenomenon, the author emphasizes the relevance of understanding by future officers the significance of countering information attacks in the process of civil-military interaction.*

Keywords: *informational warfare, future officers, Armed Forces of Ukraine, civil-military interaction.*

Анотація*. Визначаючи інформаційну війну як багатоплановий і складний феномен, автор акцентує увагу на актуальності розуміння майбутніми офіцерами значущості протидії інформаційним атакам у процесі цивільно-військової взаємодії.*

Ключові слова: *інформаційна війна, майбутні офіцери, ЗСУ, цивільно-військова взаїмодія.*

На думку української вченої О. Резнікової, причини розгортання РФ війни проти незалежної України мають не лише політичний, а й ідеологічний та історичний контексти [2]. Ще багато років тому американський соціолог З. Бжезінський акцентував увагу на тому, що "…незалежність України кинула виклик самій суті претензії Росії на те, що вона є богонатхненною прапороносицею спільної всеслов'янської ідентичності… Росія не може існувати в Європі без України, яка теж належить до Європи, тоді як Україна може бути в Європі без Росії" [1].

Джерело загроз національній безпеці, пов'язане з неефективністю системи міжнародної безпеки, виявилося особливо небезпечним саме для України, оскільки чинні механізми захисту миру та безпекові гарантії, у т. ч. за

Будапештським меморандумом [7], не завадили РФ роками здійснювати гібридну агресію проти України, а 24 лютого 2022 р. розпочати повномасштабну війну [2].

Тому, у процесі підготовки майбутніх офіцерів до цивільно-військової взаємодії протидія інформаційній війні та інформаційному тероризму розглядається одним з напрямів забезпечення інформаційної безпеки як складової частини національної безпеки країни, своєю чергою "механізми протидії зазначеним загрозам мають бути високотехнологічними та мати системний характер" [9, с. 32].

З огляду на те, що цивільно-військова взаємодія передбачає комунікацію військових з цивільним населенням, представниками місцевих/селищних рад і громадськості, які не мають військового досвіду, і та інформаційна лавина, яка щодня діє на психіку людей (різних вікових категорій), безумовно, впливає не тільки на свідомість наших громадян, а й на адекватне розуміння ситуації, в якій опинилися (як-от треба евакуюватися, заспокоїтися та ін.), тож в рамках психологічної парадигми "інформаційна війна розуміється як латентний вплив інформації на індивідуальну, групову і масову свідомість за допомогою методів пропаганди, дезінформації, маніпулювання з метою формування нових поглядів на соціально-політичну організацію суспільства через зміну ціннісних орієнтацій і базових установок особистості" [10, с. 78].

Зауважимо, що полковник Р. Шафранскі (завідувач кафедри національної військової стратегії в Повітряному військовому коледжі авіабази Максвелл, штат Алабама (США) в своїй статті "Theory of Information Warfare: Preparing For 2020" *(Теорія інформаційної війни. Підготовка до 2020)* ще в 1995 р. наголошував на тому, що інформаційна війна незалежно від того чи використовується вона безпосередньо проти зовнішнього супротивника чи внутрішніх груп, має кінцеву мету використання інформаційної зброї для впливу на системи знань і переконань деякого зовнішнього супротивника (вплив, маніпулювання, напади, психози, неврози, фобії кошмари та ін. у людей) [11, с. 4]. Тобто метою інформаційної війни є свідомість людини і, якщо ворог сконцентрований (а до 2020 року більше половини людей на планеті житиме у міських комплексах, які будуть доступні відразу у великій кількості за допомогою інформаційних технологій), інформаційну атаку можна вести проти великих груп. [11, с. 5].

Наразі інформаційний простір України перебуває під безпрецедентно потужною ворожою пропагандою, випробуючи стійкість українців перед впливом неправдивої інформації.

Український політтехнолог Д. Бачевський, характеризуючи інформаційну війну як найстрашніше і найефективніше знаряддя, що дозволяє зламати і підпорядкувати будь-яке суспільство, яке не захищається супро-

тив такого впливу, наголошує про необхідність наведення порядку в інформаційній складовій [8], бо її вплив на свідомість, підтримання морального духу українського суспільства, яке дає відсіч російському вторгненню понад 1000 днів, дуже важливе, через те що поширення панічних повідомлень і нагнітання інформації спрямовані на деморалізацію та дезорганізацію як фронту, так і тилу, формування у населення настрою безнадійності та приреченості, дискредитації військового та політичного керівництва країни, зміщення акцентів інформаційного фокусу на поразки та невдачі, хабарництво, корупцію, недостатню підтримку України нашими союзниками грають тільки на користь Росії.

До прикладу, в контексті сказаного, інформаційні пабліки протягом листопаду 2024 р. активно вводять емоційні гойдалки стосовно ядерного удару Росією по Україні: “посольства США, Італії, Греції, Іспанії зачиняються через загрозу російської атаки…”, “посольство Казахстану в Україні закликало своїх громадян…зовсім виїхати з країни”, “почалася третя світова війна”, “сьогодні може бути завдано сильного ракетного удару по Україні” (20 листопада), “про загрозу особливо масованого ракетного удару по українським містам” і додається фото з транспортуванням цієї ракети, або “РФ готує план поділу України на три частини”, “2900 людей Курахівської громади не мають бажання евакуюватися…”, одним словом, “полилося” море фейкових новин і ворожок, і пророків тощо, що не встигали спростовувати. Таких прикладів, з відповідними меседжами, які вкидаються інформаційними новинами спеціально, можна навести багато. Ким вкидаються? Не секрет, що проти нашої держави активно діють підрозділи інформаційно-психологічних операцій (ІПсО) російської армії, фсб, служби зовнішньої розвідки.

Дані, що оприлюднено Національним інститутом стратегічних досліджень стосовно вивчення стану розвитку громадянського суспільства в Україні у 2023–2024 роках наголошують на тому, що у 2023 р. в Україні спостерігалося зменшення рівня довіри до соціальних та політичних інститутів. Як наслідок, половина українців, які брали участь в опитуваннях, вважають, що громадські організації в розв’язанні соціальних проблем є набагато ефективнішими, ніж урядові та бізнесові структури [4].

Своєю чергою, ми вивчили результати соціологічного опитування, що проводилося соціологічною службою Центру Разумкова спільно з Фондом “Демократичні ініціативи” імені Ілька Кучеріва з 8 по 15 грудня 2023 року. Опитування методом face-to-face проводилося у Вінницькій, Волинській, Дніпропетровській, Житомирській, Закарпатській, Запорізькій, Івано-Франківській, Київській, Кіровоградській, Львівській, Миколаївській, Оде-

ській, Полтавській, Рівненській, Сумській, Тернопільській, Харківській, Херсонській, Хмельницькій, Черкаській, Чернігівській, Чернівецькій областях та місті Києві (у Запорізькій, Миколаївській, Харківській, Херсонській областях – лише на тих територіях, що контролюються урядом України та на яких не ведуться бойові дії). Опитано 2019 респондентів віком від 18 років. Теоретична похибка вибірки не перевищує 2,3% [5, 6].

Серед державних та суспільних інститутів найчастіше довіра висловлюється до Збройних Сил України (їм довіряють повністю 74,7% опитаних); радам міста (селища, села), в якому живе респондент відповідно 11,3%, але ЗМІ України повністю довіряють тільки 7,7% [6], що показано на таблиця 1. Причому показники балансу довіри/недовіри до названих трьох суб'єктів показує про колосальний розрив між ними: 89,1% (ЗСУ), 13,4% – місцеві ради та 4,9% (ЗМІ України), що слугує неприпустимо низькому рейтингу в умовах війни.

Також частка громадян, які вважають, що події в Україні розвиваються у правильному напрямі 45% за даними останнього опитування). 33% респондентів вважають, що події розвиваються в неправильному напрямі (21,5% не визначилися) [5].

Таблиця 1.

Якою мірою Ви довіряєте таким соціальним інститутам

Соціальні інститути	*Зовсім не довіряю*	*Скоріше не довіряю*	*Скоріше довіряю*	*Повністю довіряю*	*Важко відповісти*	*Баланс довіри/ недовіри*
Місцева рада вашого міста / селища / села	15,6	24,2	41,9	11,3	7,0	*13,4*
Збройні Сили України	2,7	1,9	19,0	74,7	1,7	*89,1*
ЗМІ України	15,1	28,1	40,4	7,7	8,7	*4,9*

Джерело складено автором за [6, с. 15]

Дані, представлені на рисунку 1, більш наочно показують безпрецедентну довіру опитаних респондентів до ЗСУ. Тож розуміння майбутніми офіцерами значущості протидії інформаційним атакам, зокрема у процесі цивільно-військової взаємодії [12–15], є актуальним, бо у тривалому протистояння проти Росії ще не напрацьовано належні механізми захисту від інформаційної війни, зі свого боку майбутня професійна діяльність офіцера ЗСУ передбачає і руйнування інформаційних систем противника.

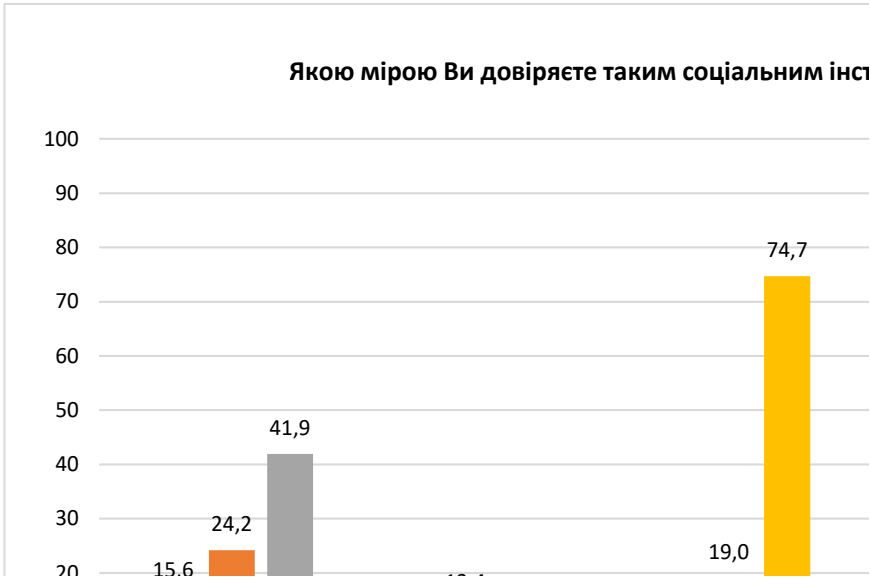


Рисунок 1 – Відповіді на запитання “Якою мірою ви довіряєтет таким соціальним інститутам? ” *Джерело:* складено автором за [6, с. 15].

Інформаційні джерела

1. Бжезінський З. (2000). Велика шахівниця. Львів – Івано-Франківськ : Лілея-НВ, 236 с.

2. Резнікова О. О. Стратегічний аналіз безпекового середовища України / Національний інститут стратегічних досліджень. Офіційний сайт. 08.09.2022. URL: https://niss.gov.ua/news/statti/stratehichnyy-analiz-bezpekovoho-seredovyshcha-ukrayiny

3. Global Cybersecurity Index 2024. 5th Edition / The International Telecommunication Union. Development Sector. Switzerland, Geneva. ITU, 2024. 151 p.

4. Стан розвитку громадянського суспільства в Україні у 2023–2024 роках / Національний інститут стратегічних досліджень. Офіційний сайт. 14.11.2024. URL: https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/stan-rozvytku-hromadyanskoho-suspilstva- v- ukrayini-u-2023–2024

5. Підсумки 2023 року: громадська думка українців /Фонд “Демократичні ініціативи” імені Ілька Кучеріва. 27 грудня 2023. URL: https://dif.org.ua/article/pidsumki-2023-roku-gromadska-dumka-ukraintsiv

6. Оцінка громадянами ситуації в країні. Довіра до соціальних інститутів, політиків, посадовців та громадських діячів / Разумков Центр. Громадська організація економічних і політичних досліджень імені Олександра Разумкова. URL:https://dif.org.ua/files/Books/2023/PDF/2_Press_release_2023_12_dovira%20(2)%D0%A6%D0%A0.pdf

7. Меморандум про гарантії безпеки у зв’язку з приєднанням України до Договору про нерозповсюдження ядерної зброї : Документ 998_158, чинний, поточна редакція – Прийняття від 05.12.1994 / Верховна Рада України. Законодавство. URL: https://zakon.rada.gov.ua/laws/show/998_158#Text

8. Бачевський Д. Українців цілеспрямовано ламають стресом. Незалежний культурологічний часопис. URL: https://www.ji-magazine.lviv.ua/2017/Bachevskyj_Ukrainciv_ svidomo_lamayut_stresom.htm

9. Носов В., Манжай О. Окремі аспекти протидії інформаційній війні в Україні. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2015. Вип. 1 (29). – С. 27–32.

10. Проноза І. І. Інформаційна війна: сутність та особливості прояву. Актуальні проблеми політики. 2018. Вип. 61. – С. 76–84.

11. Szafranski R. Theory of Information Warfare: Preparing For 2020. Airpower Journal. 1995. Spring. 14 p. URL: https://archive.org/details/5626282-Col-Richard-Szafranski-A-Theory-of-Information/mode/2up

12. Петько Л. В. Виклики XXI століття для освітнього простору України. Наукові праці ЧНУ: наук. журнал / Чорном. Нац. ун-т ім. Петра Могили; ред. кол.: О. П. Мещанінов (голова) [та ін.]. – Миколаїв: Вид-во ЧНУ імені Петра Могили, 2017. Т. 303. Вип. 291. – С. 10−14 (Педагогіка). URI : http://enpuir.npu.edu.ua/handle/123456789/18644

13. Pet'ko Lyudmila. Priorities for the development of the Ukrainian national idea and the upbringing students of this modern era. Intellectual Archive. Toronto : Shiny Word.Corp. (Canada). 2017. September/October. Vol. 6. No. 5, pp. 59−78. URI http://enpuir.npu.edu.ua/handle/123456789/16021

14. Снапкова Н. П. Підготовка майбутніх офіцерів ЗС України до цивільно-військової взаємодії. Українське військо: сучасність та історична ретроспектива: зб. матеріалів IV Міжнар. наук.-практ. конф. (м. Київ, 30 листопада 2023 р.) / Національний ун-т оборони України, Науково-дослідний центр воєнної історії навчально-наукового ін-ту воєнної історії. Київ : НУОУ, 2023. – С. 214–215

15. Снапкова Н. П. Шляхи підготовки майбутніх офіцерів Збройних сил України до цивільно-військової взаємодії. Військова освіта і наука: сьогодення та майбутнє: тези XVIII Міжнародної наук.-практ. конференції (м. Київ, 25 листопада 2022 р.) / Військовий інститут Київського нац. ун-ту імені Тараса Шевченка. Київ, 2022. – С. 191–192.

УДК 004.056

ІНФОРМАЦІЙНІ АТАКИ НА СОЦІАЛЬНІ МЕРЕЖІ

Любомир СІКОРА
Діана РУДЬКО

Кафедра автоматизованих систем управління Інституту комп'ютерних наук та інформаційних технологій Національного університету "Львівська політехніка", м. Львів, Україна.

Abstract. *This paper examines the features of information attacks on social networks. Methods of manipulating public opinion and ways of ensuring information security are analyzed.*

Keywords: *information attack, social networks, security, manipulation.*

Анотація. *У цій роботі розглянуто особливості інформаційних атак на соціальні мережі. Аналізуються методи маніпуляції суспільною думкою та способи забезпечення інформаційної безпеки.*

Ключові слова: *інформаційні атаки, соціальні мережі, безпека, маніпуляції.*

Вступ. Інформаційні атаки на соціальні мережі становлять серйозну загрозу для сучасного інформаційного простору. З розвитком цифрових технологій та Інтернету, соціальні платформи стали основним каналом для комунікацій [1], а також інструментом для розповсюдження дезінформації, впливу на суспільну думку та проведення психологічних операцій, що впливає на національну безпеку [2].

Мета і завдання дослідження. Метою дослідження є вивчення специфіки інформаційних атак на соціальні мережі, аналіз методів їх проведення та розробка рекомендацій для захисту користувачів і збереження інформаційної безпеки.

Методи дослідження. У дослідженні використовувалися методи аналізу та порівняння з наукових публікацій, а також емпіричні дані, що висвітлюють методи впливу на суспільну думку через соціальні мережі.

Результати дослідження. Соціальні мережі є головною мішенню для кіберпсихологічних атак через їх здатність швидко поширювати інформацію. Атаки націлені на створення: конфліктів і розколу в суспільстві через поширення спірних тем; паніки або недовіри до урядів через фейкові новини; підтримки певних політичних або економічних інтересів через маніпуляції громадською думкою.

Погроза поширення конфіденційної інформації через програми вимагачі. Програми-вимагачі стають загрозою не лише для великих компаній, а й для користувачів соціальних мереж. Вони можуть бути інструментом масових інформаційних атак, спрямованих на поширення шкідливого програмного забезпечення через соціальні платформи. Зловмисники поширюють шкідливі посилання або файли через фейкові облікові записи та обманним шляхом змушують користувачів завантажити програми-вимагачі. Такий підхід дозволяє залучити широке коло користувачів до атаки, адже соціальні мережі мають величезне охоплення. Для організацій, які активно використовують соціальні мережі для взаємодії з клієнтами, загроза ще більша. У випадку зараження через сторінки в соціальних мережах, їхні акаунти можуть бути заблоковані, а дані клієнтів – викрадені. Це загрожує репутації компанії, втратою довіри користувачів та судовими позовами.

Окрім того, такі атаки часто супроводжуються вимогою викупу за розблокування акаунтів або повернення даних, що створює додатковий фінансовий тягар для організацій. У результаті активності кіберзлочинних угруповань, що поширюють програми-вимагачі через соціальні мережі, кількість кіберзлочинів в загальному зростає. Це вимагає від користувачів та компаній підвищеної обережності та впровадження ефективних заходів для захисту своїх цифрових активів у соціальних платформах.

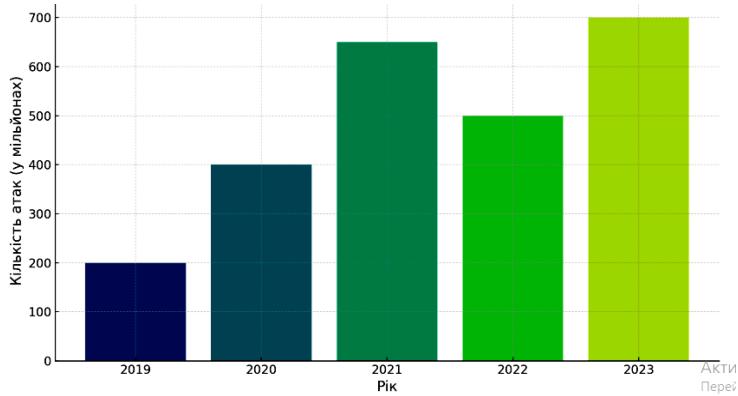


Рисунок 1 – Зміна кількості програм вимагачів (2019–2023)

Технології штучного інтелекту для маніпуляції. Штучний інтелект (AI) та глибокі фейки (deepfake) стають потужними інструментами для маніпуляції. Використовуючи алгоритми AI, можна створювати фальшиві відео або аудіо, які виглядають дуже реалістично, і поширювати їх у соціальних мережах для впливу на масову свідомість [3].

Цифрова обробка сигналів у контексті виявлення кіберзагроз. Одним із ключових аспектів протидії кіберпсихологічним атакам є застосування методів цифрової обробки сигналів. Вони дозволяють аналізувати великі обсяги даних та виявляти потенційні загрози. Цифрова обробка сигналів є критично важливою для виявлення та протидії кіберпсихологічним атакам, проте вона стикається з кількома серйозними викликами.

Обробка великих обсягів даних. Сучасні інформаційні системи генерують величезні обсяги даних щодня. Ці дані можуть містити інформацію про поведінку користувачів в інтернеті, мережевий трафік та інші важливі параметри. Основною проблемою є здатність аналізувати ці дані в реальному часі, щоб виявити потенційні загрози. Традиційні системи обробки даних часто не справляються з такими обсягами, що веде до затримок у виявленні загроз.

Складність виявлення дезінформації. Визначення того, що є правдою, а що є дезінформацією, стає дедалі складнішим завданням. Використання алгоритмів машинного навчання може допомогти у виявленні фейкових новин, але ці алгоритми не завжди точні і можуть давати хибні спрацьовування. Часто дезінформація створюється на основі правдивих фактів, що ускладнює її виявлення.

Проблеми з конфіденційністю. Використання технологій для моніторингу інформаційного простору ставить питання про конфіденційність даних. Баланс між безпекою та правами людини є складним завданням, яке потребує чіткої правової бази. Держава повинна знайти способи захисту своїх громадян від дезінформації, не порушуючи їхні права на приватність.

Таблиця 1.

Технології цифрової обробки сигналів у сфері кібербезпеки

Технологія	*Опис та застосування*	*Приклад використання*
Штучний інтелект (AI)	Автоматизоване виявлення патернів та аномалій у інформаційних потоках	Виявлення ботів у соціальних мережах
Машинне навчання (ML)	Алгоритми, що навчаються на основі даних для прогнозування атак	Прогнозування кіберпсихологічних атак
Нейронні мережі	Аналіз великих даних для виявлення складних загроз	Виявлення глибоких фейків (deepfake)
Аналіз мережевого трафіку	Аналіз трафіку для виявлення аномалій у комунікаційних потоках	Виявлення DDoS-атак та підозрілої активності
Обробка сигналів (DSP)	Фільтрація та аналіз сигналів для виявлення кіберзагроз	Фільтрація спаму, захист від фейкових новин

Методи обробки та фільтрації сигналів у кібербезпеці. Обробка цифрових сигналів дозволяє ефективно: виявляти аномалії у мережевих потоках, які можуть вказувати на проведення кібер психологічної атаки; фільтрувати зловмисні сигнали, що походять від ботів чи шкідливих програм; аналізувати соціальні мережі для виявлення координованих інформаційних кампаній.

Системи моніторингу мережевої активності. Системи цифрової обробки сигналів використовуються для моніторингу інтернет-трафіку, щоб ідентифікувати потенційні загрози в реальному часі, допомагаючи виявляти фейкові новини, боти та інші форми маніпуляції.

У цьому дослідженні було розглянуто, як цифрові технології та обробка сигналів змінили підхід до ведення психологічних війн у сучасну епоху. Наступні досідження будуть присвячені розгляду питань підвищення національної безпеки в контексті протидії інформаційним атакам.

Висновки. Інформаційні атаки на соціальні мережі є значною загрозою, що вимагає об'єднання зусиль держав, технологічних компаній та користувачів для запобігання маніпуляціям і захисту інформації. Важливим кроком підвищення інформаційної безпеки є посилення цифрової грамотності користувачів соціальних мереж та вдосконалення алгоритмів виявлення підозрілих активностей.

Інформаційні джерела

1. Березовська Л. Вплив соціальних мереж на психологічне благополуччя особистості. Вісник Національного університету оборони України. 2020. 55. – С. 28–36. doi: 10.33099/2617-6858-2020-55-2-28-36.

2. Карпенко В. Інформаційний простір як чинник національної безпеки. Українознавство. 2005. № 3. – С. 182–192.

3. Крикун В., Бауліна Т. Дезінформація як засіб гібридної війни: сутність і наслідки. Вісник Київського національного університету імені Тараса Шевченка. Філософія. 2022, Вип. 2. – С. 30–33.

Секція 2

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ ВІЙНИ

Напрям 9

ПРИКЛАДНЕ ТА СИСТЕМНЕ ПРОГРАМУВАННЯ

UDC: 004.4

SERVER LOAD BALANCING MATHEMATICAL MODEL BASED ON AUTOMATIC NODE'S RATING EVALUATION

Taras MILIANETS
Andrii PUKACH
Lviv Polytechnic National University, Lviv, Ukraine.

Анотація. *В епоху стрімкого технологічного прогресу, зростання даних і запитів до серверів вимагає ефективних механізмів розподілу навантаження. У цьому дослідженні пропонується модель динамічного балансування навантаження, яка використовує показники в реальному часі, включаючи час відповіді, активні з'єднання, використання процесора та споживання оперативної пам'яті, для оптимізації розподілу ресурсів між серверами.*

Ключові слова: *Динамічне балансування навантаження, метрики в реальному часі, система рейтингу вузлів, нормалізовані параметри, розподілені системи, масштабованість, оптимізація продуктивності.*

Abstract *In the era of rapid technological advancement, the growth in data and server requests necessitates efficient load distribution mechanisms. This study proposes a dynamic load balancing model that leverages real-time metrics including response time, active connections, CPU usage, and RAM consumption to optimize resource distribution across servers.*

Keywords: *Dynamic load balancing, real-time metrics, node rating system, normalized parameters, distributed systems, scalability, performance optimization.*

Problem Statement. In the conditions of technological development, the amount of data and requests to servers and computer systems is growing in geometric progression. In order to meet high standards of reliability and availability, it is important to efficiently distribute the load between servers or other components. The load on the servers is unpredictable as user requests may vary in amount and complexity.

Traditional static load balancing methods can`t provide efficient distribution of the requests which can lead to bottlenecks and inefficient resource utilization. Common approaches to load balancing use algorithms such as Round Robin, Least Connections, and Weighted Round Robin [1]. These algorithms distribute requests between servers, taking into account a limited number of factors, such as

the number of active connections or a simple round-robin distribution of requests. Although these methods are effective for small systems and relatively stable loads, they face serious challenges in today's highly loaded and dynamic systems. Most often, such approaches are not able to quickly adapt to changes in requests, due to which the system may have delays in responses or even failures in cases of overloading of individual nodes.

To solve these problems, dynamic load balancing approaches [2] are considered, which allow the system to adapt to changes in real time, ensuring the optimal distribution of resources. The basic idea behind dynamic balancing [3] is to continuously monitoring system performance metrics, such as CPU usage, memory consumption, and network bandwidth. This allows the system to effectively distribute user requests between available nodes based on real-time data.

Proposed Solution. In this research a load balancing mathematical model is being developed, based on each node's rating, which is calculated from real-time metrics. To calculate the rating of each node, this model takes into account the main indicators: response time, number of connections and resource consumption. Each of these parameters can be weighted to reflect their importance in the overall assessment. The lower the rating, the higher the readiness of the node to serve new requests.

Rating calculation model for load balancing:

Collect indicators for each node:

R – the average response time

C – the number of active connections

CPU – *CPU* load level (in percent)

RAM – *RAM* usage (in percent)

Normalize the parameter values:

Let's reduce the value of each indicator to the range [0, 1] to simplify the comparison. Normalization [4] of parameter P is carried out according to the formula:

$$X_{normalized} = \frac{P - P_{\min}}{P_{\max} - P_{\min}} \qquad (1)$$

Where P – is the parameter value for a specific node, $P_{\min}$ and $P_{\max}$ – the minimum and maximum value of this parameter among all nodes.

Calculate the rating for each node:

The rating is calculated as a weighted sum of normalized parameter values.

Formula for rating:

$$Node\ Rating = \omega_R \cdot R_{normalized} + \omega_C \cdot C_{normalized} + \omega_{CPU} \cdot \cdot CPU_{normalized} + \omega_{RAM} \cdot RAM_{normalized} \qquad (2)$$

Where $\omega_R, \omega_C, \omega_{CPU}, \omega_{RAM}$ – weights for each parameter. Weights are determined based on the importance of each indicator in the system. For example, if the CPU is critical, you can give it more weight. For example, the weights can be distributed as follows:

$$\omega_R = 0.2,\ \omega_C = 0.2,\ \omega_{CPU} = 0.4,\ \omega_{RAM} = 0.2$$

Selecting a node to serve requests:

After calculating the rating for all nodes, we choose the node with the lowest rating, because it has the least load and is the most ready to process new requests.

This model allows you to flexibly and dynamically distribute the load depending on the current state of the nodes, ensuring optimal use of resources and uniform load of the entire system.

Conclusion. The scientific novelty of the proposed model lies in improvement of the existing methods for load balancing by providing flexibility in parameters selection and their importance in rating calculation. The model takes into account a complex set of indicators and has advantages over traditional static approaches, which ensures a more accurate distribution of requests and high adaptability to changes in the load. Dynamic balancing using the rating of each node helps to reduce delays, increase the performance and reliability of systems, which positively affects the user experience and meets the requirements of modern highly loaded distributed infrastructures.

Information sources

1. Chaubey D. (n.d.). Types of load balancing algorithms. OpenGenus IQ: Learn Algorithms, DL, System Design. URL: https://iq.opengenus.org/load-balancing-algorithms/

2. Gunasekaran S., & Deepa M. (2021). Load Balancing Techniques in Cloud Computing: Extensive Review. Advances in Science, Technology and Engineering Systems Journal, 6(2), pp. 1001–1007. URL: http://dx.doi.org/10.25046/aj060299

3. Laha J., Pattnaik S., & Chaudhury K. S. (2024). Dynamic Load Balancing in Cloud Computing: A Review and a Novel Approach. EAI Endorsed Transactions on Internet of Things, 10. URL: https://doi.org/10.4108/eetiot.5387

4. DataCamp. (n.d.). What is normalization in machine learning? A comprehensive guide to data rescaling. DataCamp. URL: https://www.datacamp.com/tutorial/ normalization-in-machine-learning

5. Ray S., & De Sarkar A. (2021). Execution analysis of load balancing algorithms in cloud computing environment. International Journal on Cloud Computing: Services and Architecture (IJCCSA), 2(5). URL: https://doi.org/10.5121/ijccsa.2012.2501

Swarnakar S., Kumar R., & Krishn S. (2020). Improved dynamic load balancing approach in cloud computing. 2020 IEEE International Conference for Convergence in Engineering. pp. 42–47. URL: https://doi.org/10.1109/ICCE50343.2020.9290602

УДК 004.43

SURVEY OF DSL GENERATORS FOR THE JAVA PLATFORM

Vladyslav BILYK

IT STEP University, Lviv, Ukraine.

Анотація. *Робота аналізує генератори DSL для Java, їхню ефективність у вирішенні проблем розробки DSL, гнучкість і підтримку різних граматик. Розглянуто обмеження існуючих рішень і запропоновано рекомендації для вибору та створення ефективних інструментів для розробки DSL.*

Ключові слова: *мова програмування Java, предметно-орієнтовні мови програмування, генерування програмного коду.*

Abstract. *This paper analyzes DSL generators for Java, evaluating their effectiveness in addressing DSL development challenges, flexibility, and grammar support. The study identifies limitations of existing solutions and provides recommendations for selecting and developing efficient DSL tools.*

Keywords: *Java programming language, domain-specific languages, source code generation.*

Domain-Specific Languages (DSLs) are programming languages tailored to specific problem domains, with specialized syntax and semantics. Unlike general-purpose languages (GPLs), which are broadly applicable, DSLs excel at expressing domain-specific solutions concisely and clearly. Common examples include SQL, HTML, and regular expressions. By providing high-level abstractions aligned with domain concepts, DSLs reduce boilerplate code, enhance expressiveness, and improve maintainability. However, creating and maintaining DSLs can be complex, requiring expertise in grammar design, parser implementation, and system integration, with additional costs for adaptation to evolving domain requirements.

In Java, DSLs often take the form of fluent APIs, which use method chaining and expressive names to create domain-like constructs within Java's boundaries. Internal DSLs, embedded in a host language like Java, inherit its benefits, such as type safety, IDE support, and a rich software ecosystem. DSL generators automate much of the manual effort involved in DSL creation by producing a fluent API, a parser, and an AST based on a DSL description. While these tools reduce development time and simplify maintenance, they also have drawbacks such as limited customizability and potential complexity in the generated code.

The aim of this work is to evaluate the effectiveness of DSL generators based on three primary criteria: User Interface, Generated Fluent API, and Generated AST. These criteria are derived from the key goals of DSL generation: ease of use, quality of the generated code's structure, and efficiency of the generated code.

1. User Interface: DSL generators typically accept a description of a DSL as input, often expressed as a grammar in the Backus-Naur Form (BNF). For this assessment, we focus on context-free grammars (CFGs), particularly those supporting left recursion due to their natural, top-down structure. A generator's ability to handle left-recursive grammars is a baseline requirement for usability. Generators that demand extensive rewriting of grammars by users fall short. Additionally, allowing users to specify documentation for the generated code is a valuable, optional feature.

2. Generated Fluent API: The fluent API, a key output of a DSL generator, serves as the interface for interacting with the DSL. It should closely align with the input grammar to ensure consistency and avoid overly complex constructs that could slow down the compiler or affect IDE performance. The generated API must also include a parser implementation that is efficient in terms of time and space.

3. Generated AST: The generated AST represents the DSL's structure and is crucial for tasks like creating interpreters. The generator should produce an AST that aligns closely with the input grammar. A flexible user interface that imposes minimal restrictions on input grammars is essential for generating ASTs that are intuitive and easy to use. Restrictive input requirements can hinder the usability of even a well-aligned AST.

Three notable DSL generators for Java were examined in this work: Fling, Silverchain, and Flapi. Each of these tools is described and assessed based on the established criteria.

1. Fling is a fluent API generator that accepts an LL(1) grammar as BNF or a deterministic push-down automaton (DPDA) description [1]. It generates a fluent API, a parser, and an AST.

User Interface: Fling cannot handle left-recursive grammars due to its restriction on input that is required to be an LL grammar.

Generated Fluent API: The generated code heavily uses type parameterization, enabling DSL generation but leading to complexity in cases where much nesting occurs.

Generated AST: Fling produces an AST closely aligned with the input grammar, but the restriction to LL inputs can obscure the resulting structure.

2. Silverchain is a fluent API generator notable for providing an external DSL as input [2].

User Interface: Instead of accepting a grammar, Silverchain uses a Java-like DSL equivalent to regular expressions, which excludes left-recursive grammars.

Generated Fluent API: The generated API reflects the input's complexity but avoids excessive type parameterization, resulting in simpler APIs. It also supports embedding documentation into the API, contributing to maintainability.

Generated AST: Silverchain does not produce an AST or its implementation, focusing solely on a fluent API.

3. Flapi is a fluent API generator that offers both an internal DSL and annotation-based input mechanisms [3].

User Interface: Inputs are limited to the expressivity of regular grammars, with descriptions provided either as a fluent API or Java annotations.

Generated Fluent API: The generated APIs are simple and straightforward due to Flapi's limited expressivity. Documentation embedding is supported.

Generated AST: Flapi does not generate an AST, reducing its scope of application.

This work examined DSL generation for the Java platform, analyzing its challenges and effectiveness of available solutions. Three popular DSL generators were evaluated: Fling, Silverchain, and Flapi, using the criteria of user interface flexibility and generated code quality.

Fling is the most powerful tool, producing precise ASTs and complete fluent APIs but is limited to LL grammars and lacks support for embedding documentation. Silverchain streamlines API generation with documentation support but does not generate ASTs, limiting its utility. Flapi focuses on fluent API generation, offering internal DSL and annotation-based input but also lacks AST generation.

Conclusion. In conclusion, while DSL generators are valuable tools for DSL development, each has constraints that influence their applicability in different scenarios. Understanding these capabilities helps developers make informed decisions.

Information sources

1. Yossi Gil and Ori Roth. "Fling – A Fluent API Generator". In 33rd European Conference on Object-Oriented Programming (ECOOP 2019). Leibniz International Proceedings in Informatics (LIPIcs), Volume 134, pp. 13:1–13:25, Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2019). doi: 10.4230/LIPIcs.ECOOP.2019.13.

2. Tomoki Nakamaru, Kazuhiro Ichikawa, Tetsuro Yamazaki, and Shigeru Chiba. "Silverchain: a fluent API generator". GPCE 2017: Proceedings of the 16th ACM SIGPLAN International Conference on Generative Programming: Concepts and Experiences, pp. 199–211. doi: 10.1145/3136040.3136041.

3. Benjamin Fagin, Flapi – A fluent API generator for Java. URL: https://github.com/UnquietCode/Flapi.

УДК: 004.9:614.8

РОЗРОБЛЕННЯ ПРОГРАМНОЇ СИСТЕМИ ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ СИЛ ТА ЗАСОБІВ ДЛЯ ГАСІННЯ ПОЖЕЖІ В ФОРМАТІ ЧАТ-БОТА

Олег КІСІЛЬ
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The paper examines the development of a software system in the form of a chatbot designed to determine the optimal forces and means for firefighting. The architecture, data processing algorithms, and main functionalities of the chatbot are presented. The proposed approach enhances decision-making efficiency and speed in the firefighting domain through automated calculations and real-time data provision.*
Keywords: *chatbot, firefighting, optimization, data processing, information systems.*

Анотація. *У роботі розглянуто процес розробки програмної системи у вигляді чат-бота, яка забезпечує визначення оптимальних сил і засобів для гасіння пожежі. Представлено архітектуру системи, алгоритми обробки даних та основні функціональні можливості чат-бота. Запропонований підхід дозволяє підвищити ефективність і швидкість прийняття рішень у пожежній сфері за рахунок автоматизації обчислень та оперативного надання інформації.*
Ключові слова: *чат-бот, гасіння пожежі, оптимізація, обробка даних, інформаційні системи.*

Інформаційні технології активно впроваджуються у сферу пожежної безпеки. Зростає потреба у створенні автоматизованих рішень, які допомагають швидко оцінити необхідні ресурси для ліквідації пожеж. У роботі запропоновано розроблення системи у вигляді чат-бота, який оптимізує процес розрахунків та підвищує оперативність реагування.

Постановка завдання

Метою дослідження є створення програмного забезпечення у вигляді чат-бота для автоматизації процесу визначення оптимальних сил і засобів для гасіння пожежі.

Основні вимоги до системи:

– точність обчислень на основі вихідних параметрів пожежі;

– зручність і доступність для користувачів;

– інтеграція з зовнішніми системами;

– можливість врахування особливих характеристик об’єктів і пожеж.

Архітектура системи

Система складається з таких компонентів:

– модуль збору даних: обробляє введені користувачем дані (тип об’єкта, площа пожежі, час прибуття підрозділів тощо);

– база даних: зберігає інформацію про типи об’єктів, вогнегасники, алгоритми розрахунків;

– алгоритмічний модуль: реалізує методи розрахунку кількості сил і засобів на основі формул та статистичних моделей;

– інтерфейс користувача: забезпечує взаємодію через Telegram-бот.

Алгоритми роботи

Процес визначення оптимальних сил і засобів включає такі етапи:

– збір вихідних даних: площа, тип об'єкта, час вільного розвитку пожежі;

– виконання розрахунків: обчислення необхідної кількості технічних засобів і персоналу;

– надання рекомендацій: виведення результатів у вигляді текстових повідомлень.

Для розрахунків використовуються формули, що враховують радіус, площу та інтенсивність пожежі.

Реалізація та тестування

Система реалізована на основі таких технологій:

– Back-end: Python (бібліотека Telebot);

– інтерфейс: Telegram API.

Тестування проводилося на моделях реальних пожежних сценаріїв. Результати показали високу точність розрахунків (понад 90%) і швидкість обробки запитів (менше 1 секунди).

Висновки. Розроблений чат-бот забезпечує оперативність у прийнятті рішень під час пожеж. Система демонструє високу ефективність та може бути інтегрована у практичну діяльність підрозділів ДСНС. Подальший розвиток включатиме персоналізацію рекомендацій та розширення функціоналу для роботи з різними типами надзвичайних ситуацій.

Інформаційні джерела

1. Рамальо Л. Fluent Python: Чітке, стисле та ефективне програмування. O'Reilly Media, 2015.

2. Практикум з курсу "Пожежна тактика". Львів: ЛДУБЖД, 2008.

3. Documentation. Telegram API. URL: https://core.telegram.org/bots.

УДК 004.[6+8]

ДОСЛІДЖЕННЯ МЕТОДІВ ОБРОБКИ СИГНАЛУ PPG ДЛЯ ВИЯВЛЕННЯ ТА УСУНЕННЯ ВИКИДІВ

Олена ЛІТОВСЬКА

Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *In this paper, the methods of processing photoplethysmogram signals, which were obtained using Samsung Galaxy 5 smartwatches with a frequency of 25 Hz, were investigated. The main goal is to detect and eliminate anomalies in PPG signals. Outlier detection methods were used, the best results of which were shown by the DBSCAN method. The methods of bandwidth filtration are analyzed, of which the Butterworth filter showed the best results.*

Keywords: *photoplethysmogram (PPG), outliers, STD, IQR, DBSCAN, bandpass filters, Butterworth filter, Chebyshev filters of the I and II types, elliptic filter, Kolmogorov-Smirnov criterion, logarithmic transformation, heart rate, blood oxygen level (SpO2), stress level.*

Анотація. *У цій роботі досліджено методи обробки сигналів фотоплетизмограми, які отримані з використанням смарт-годинників Samsung Galaxy 5 з частотою 25 Гц. Основною метою є виявлення та усунення аномалій у сигналах PPG. Застосовано методи виявлення викидів, найкращі результати з яких показав метод DBSCAN. Проаналізовано методи смугової фільтрації, з яких фільтр Butterworth показав найкращі результати.*

Ключові слова: *фотоплетизмограма, викиди, стандартне відхилення, міжквартильний розмах, кластеризація на основі щільності, смугові фільтри, фільтр Баттерворта, фільтри Чебишева I та II типу, еліптичний фільтр, критерій Колмогорова-Смірнова, логарифмічне перетворення, частота серцевих скорочень, рівень кисню в крові (SpO2), рівень стресу.*

Актуальність. Фотоплетизмографія – це оптичний метод вимірювання. Він використовується для виявлення змін в об'ємі крові у мікросудинах шкіри. Якість та точність цього сигналу є особливо важливими у медичних вимірюваннях, оскільки їх застосовують для моніторингу серцевого ритму, насичення крові киснем (SpO2) та інших офізіологічних показників. Це є важливим інструментом для оцінки психофізіологічного стану працівників на промислових підприємствах.

Проблема. Спотворення у сигналах PPG можуть мати вагомі медичні наслідки, адже неправильні дані можуть призвести до помилкових діагнозів або ж неправильних рішень щодо поточного стану здоров'я людини. Похибки у даних можуть виникати з різних причин, серед яких рух тіла, неправильне розташування датчика або навіть зовнішні електромагнітні завади. Якість сигналу може залежати також від віку людини. Різні види захворювань та інших фізіологічних станів теж можуть мати вагомий вплив. Це призводить до значної невідповідності до нормального розподілу, що ускладнює точну оцінку фізіологічних параметрів (рис. 1).

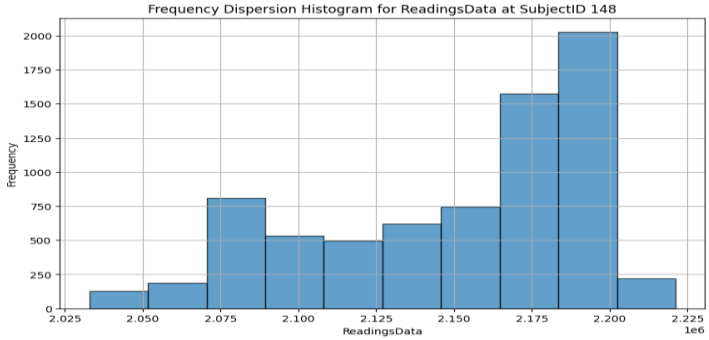


Рисунок 1 – Гістограма розподілу PPG-сигналу

Виклад основного матеріалу. Для виявлення викидів у сигналах PPG було використано 3 методи: STD, IQR та DBSCAN. Зібрані дані не відповідають нормальному розподілу, що підтверджується тестом Колмогорова-Смірнова. Середнє значення статистики Колмогорова-Смірнова для всіх записів становить 0.10197996501706467, максимальне значення P-значення – 4.93e-05, мінімальне P-значення – 0.0, максимальне значення статистики Колмогорова-Смірнова – 0.19992, а мінімальне – 0.029. Тому методи STD та IQR не підходять навіть після логарифмічного перетворення (рис. 2).

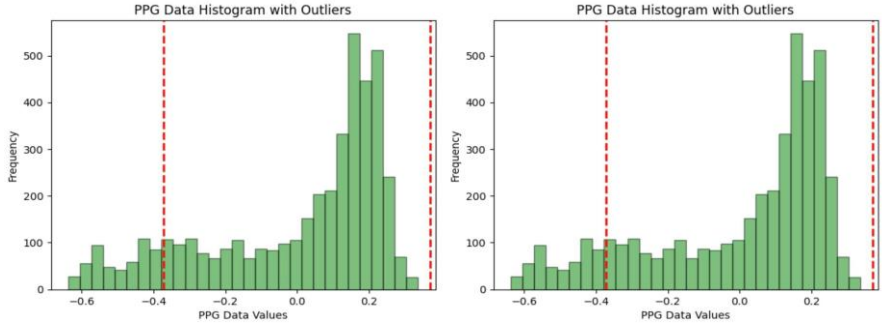


Рисунок 2 – Результати методу STD на даних до та після логарифмічної трансформації

Щоб виявити викиди за допомогою DBSCAN, було здійснено пошук найкращих значень параметрів. Вони визначають максимальну відстань між двома точками, щоб одна з них вважалася сусідом іншої, та мінімальну кількість точок, які повинні знаходитися в околиці точки, щоб ця точка вважалася “ядром” кластера. Автоматично підібрано і протестовано 216 комбінацій цих параметрів. Найоптимальніших результатів досягнуто при максимальному радіусі 0.003 та мінімальній кількості сусідів 19. Ця комбінація показала відсоток викидів 0.5% та різницю Z-оцінок до та після видалення викидів (з 3.72 до 3.57). Порівняння методів зображено на рисунок 3. Важливо зазначити, що перед застосуванням методів виявлення викидів було проведено нормалізацію та детрендінг.

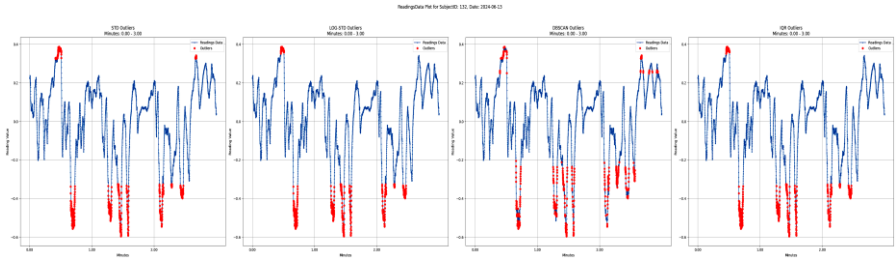


Рисунок 3 – Результати пошуку викидів за допомогою методів STD, STD з логарифмічною трансформацією, DBSCAN та IQR

Після знаходження викидів, застосовано метод ковзного середнього (рис. 4). Для визначення оптимального параметра розміру вікна було підібрано значення у діапазоні від 4 до 30. Було виявлено, що розмір вікна від 4 до 12 є недостатнім для ефективного згладжування викидів. З іншого боку, розмір вікна від 20 до 30 призводив до значного викривлення даних, що якраз зображено на графіку. Отже, було обрано розмір вікна 14, оскільки він забезпечує оптимальний баланс між ефективним згладжуванням викидів і мінімальним викривленням даних.

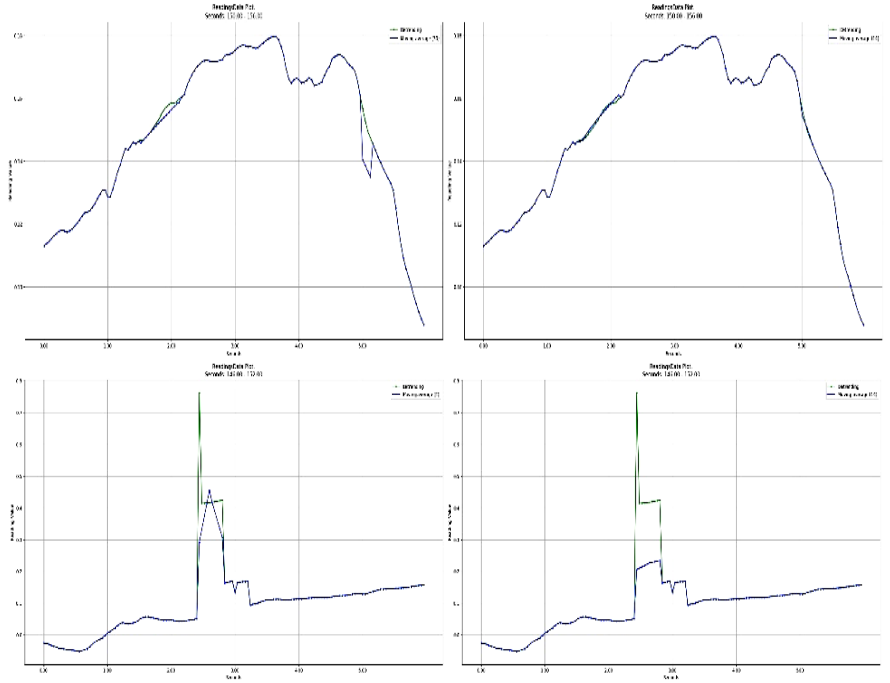


Рисунок 4 – Метод ковзного середнього з розміром вікна = 4 і 14 (синя лінія)

У цьому дослідженні було проаналізовано кілька методів смугової фільтрації, зокрема фільтр Butterworth, еліптичний, Чебишева I та II типів (рис. 5). Фільтр Butterworth має гладку амплітудно-частотну характеристику без коливань у смугах пропускання та згасання, що робить його універсальним для багатьох застосувань, включаючи біомедичний аналіз сигналів. Після оцінки методів смугової фільтрації було обрано фільтр Butterworth. Основною причиною цього вибору є його здатність забезпечувати гладку амплітудно-частотну характеристику без значних коливань, що має вагоме значення для точного аналізу сигналу PPG.

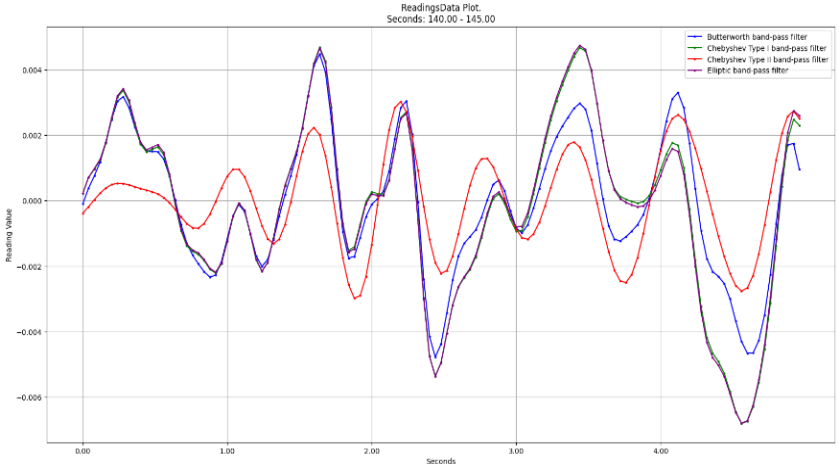


Рисунок 5 – Порівняння смугових фільтрів на сигналі PPG: Butterworth, еліптичний, Чебишева I та II типів

Висновки. Результати демонструють, що поєднання методу DBSCAN для виявлення викидів, методу ковзного середнього для усунення викидів і фільтра Butterworth для смугової фільтрації ефективно покращує якість сигналів PPG. Це підвищує надійність і точність аналізу PPG-сигналів, сприяючи більш точним фізіологічним вимірюванням і виявленню аномалій.

Подальші дослідження будуть спрямовані на вдосконалення методів обробки сигналу PPG та розробку нових алгоритмів для точного розрахунку частоти серцевих скорочень, рівня кисню в крові та рівня стресу. Це необхідно для відслідковування психофізичного стану працівників промислових підприємств, що дозволить своєчасно виявляти ознаки перевтоми, стресу або інших небезпечних станів.

Інформаційні джерела

1. Azam Siti, Nurfarah Ain and Sidek Khairul Azami and Ismail Ahmad Fadzil (2018) Photoplethysmogram based biometric identification incorporating different age and gender group. Journal of Telecommunication, Electronic and Computer Engineering, 10 (1–5), pp. 101–108. ISSN 2180-1843 E-ISSN 2289-8131.

2. Shafique M., Kyriacou P. A., and Pal S. K., “Investigation of photoplethy smographic signals and blood oxygen saturation values on healthy volunteers during cuff-induced hypoperfusion using a multimode PPG/SpO 2 sensor,” Medical and Biological Engineering and Computing, vol. 50, no. 6, pp. 575–583, 2012. URL: https:// doi.org/ 10.1007/s11517-012-0910-z.

3. Budidha K. and Kyriacou P. A. “In vivo investigation of ear canal pulse oximetry during hypothermia,” Journal of Clinical Monitoring and Computing, vol. 32, no. 1, pp. 97–107, 2018. URL: https://doi.org/10.1007/s10877-017-9975-4.

4. Chatterjee S. and Kyriacou P. A., “Monte carlo analysis of optical interactions in reflectance and transmittance finger photoplethysmography,” Sensors, vol. 19, no. 4, 2019. URL: https://doi.org/10.3390/s19040789.

5. Chatterjee S., Budidha K., and Kyriacou P. A., “Investigating the origin of photoplethysmography using a multiwavelength Monte Carlo model,” Physiological Measurement, vol. 41, no. 8, p. 084001, 2020. URL: https://doi.org/10.1088/1361-6579/aba008.

6. Moco A. V., Stuijk S., and De Haan G., “New insights into the origin of remote PPG signals in visible light and infrared,” Scientific Reports, vol. 8, no. 1, pp. 1–15, 2018. URL: https://doi.org/10.1038/s41598-018-26068-2.

7. Kamshilin A. A. and Margaryants N. B., “Origin of photoplethysmographic waveform at green light,” Physics Procedia, vol. 86, pp. 72–80, 2017. URL: https://doi.org/10.1016/j.phpro.2017.01.024.

УДК 004.[6+8]

СИСТЕМА ЗБОРУ ТА ПРЕПРОЦЕСИНГУ ДАНИХ ТРИОСЬОВИХ АКСЕЛЕРОМЕТРА ТА ГІРОСКОПА ОТРИМАНИХ ЗА ДОПОМОГОЮ СМАРТ-ГОДИННИКІВ

Олена ПАВЛЮК
Анастасія ЗАБОЛОТНА
Мирослав МІЩУК
Національний університет “Львівська політехніка”, м. Львів, Україна.

Abstract. *The use of smart watches to collect data from three-axis accelerometers and gyroscopes in an industrial environment is investigated. To reduce the impact of noise and restore partially lost data, filtering and smoothing methods were applied, among which local regression demonstrated the highest efficiency. The proposed approach will provide an accurate analysis of personnel movements, increasing the efficiency of production processes, and creates a basis for the implementation of neural network systems for recognizing types of human activity.*

Keywords: *smart watch, preprocessing, cloud database, accelerometer, gyroscope, filter, moving average, exponential smoothing, local regression.*

Анотація. *Досліджено використання смарт-годинників для збору даних з триосьових акселерометрів і гіроскопів у промисловому середовищі. Для зниження впливу шуму та відновлення частково втрачених даних застосовано методи фільтрації та згладжування, серед яких локальна регресія продемонструвала найвищу ефективність. Запропонований підхід забезпечить точний аналіз рухів персоналу, підвищуючи ефективність виробничих процесів, і створює основу для впровадження нейромережевих систем розпізнавання видів людської діяльності.*

Ключові слова: *смарт-годинник, препроцесинг, хмарна БД, акселерометр, гіроскоп, фільтр, ковзне середнє, експоненційне згладжування, локальна регресія.*

Актуальність. Розпізнавання людської діяльності (РЛД) – галузь досліджень, яка набула особливого значення завдяки широкому впровадженню носимих технологій. Практичні застосування РЛД охоплюють найрізноманітніші сфери. У галузі охороні здоров'я РЛД використовується для детекції та запобігання падінь, виявлення епілептичних нападів і моніторингу фізичної активності [1–4]. Застосування у галузі безпеки включають розпізнавання аномальної діяльності [5]. У спорті РЛД використовується для оцінок ефективності тренувань і витрати калорій [6, 7].

В епоху Індустрії 4.0 і поточного переходу до Індустрії 5.0 виникло нове поле для застосувань РЛД, яке включає такі задачі як оцінка добробуту персоналу та інтелектуальне управління підприємством [8]. Сьогодні збір даних у більшості існуючих систем на промислових підприємствах здійснюють за допомогою камер. Проте такі методи мають ряд обмежень, зокрема через кут зору камер. Тому накладаються обмеження на траєкторії пересування персоналу.

В даних дослідженнях запропоновано здійснювати збір даних за допомогою сенсорів смарт-годинників, які не накладають обмежень на рух персоналу [9]. Більше того, вони не заборонені до використання нормами охорони праці для працівників промислових підприємств. Всі дослідження проводили за допомогою Samsung Galaxy 5. Проте при зборі даних через певні фізичні явища вони можуть випадковим чином бути відсутні, чи містити шуми.

Це може відбуватися через фізичні обмеження сенсорів:

– обмежений діапазон, якщо акселерометр або гіроскоп перевищують діапазон вимірювань – тоді дані стають некоректними.

– теплові ефекти, коли сенсори іноді можуть давати не точні результати через коливання температур.

Шум у даних:

– високий рівень шуму, якщо дані з акселерометра та гіроскопа часто містять шум через фізичні впливи. Вібрації, спотворення траєкторій та ін. утворюють шум, що може значно погіршити точність вимірювань.

– зовнішні впливи: не механічні спотворення спричинені магнітними полями чи електричними перешкодами і можуть також викликати непередбачувані зміни сигналу сенсора, збільшуючи кількість шуму і знижуючи надійність даних.

Мережеві збої: у системах збору та передачі інформації по мережі за допомогою акселерометрів та гіроскопів, що є у смарт-годинниках, можуть бути програмні чи апаратні збої, які можуть спричинити затримку або втрату даних. Це призводить до відсутності оновлень про рух або положення об'єкта у просторі. Для складних систем це може означати втрату важливої інформації про рух об'єкта, що пізніше призведе до помилок у керуванні.

Проблема. Важливою проблемою є збір інформації зі смарт-годинників та її попередня обробка, яка включає: виявлення та відновлення частково втрачених даних за допомогою фільтрів.

Мета. Метою досліджень є розроблення ефективної системи збору інформації зі смарт-годинників персоналу і її попередня обробка для подальшого аналізу та прогнозу на промислових підприємствах.

Виклад основного матеріалу

Збір даних з смарт-годинників Samsung Galaxy Watch 5 виконується за допомогою розробленої апаратно-програмної системи сумісної з операційною системою WearOS. Для розробки застосунку використовувалася мова програмування Kotlin для операційних систем WearOS та AndroidOS. Застосунок призначений для збору даних зі сенсорів триосьових акселерометра і гіроскопа та їх передачі на хмарний сервер, який базується на MySQL. Також він забезпечує інтерфейс для управління процесом збору даних.

На рисунку 1 показані основні екрани користувацького інтерфейсу розробленого застосунку для смарт-годинника показані. Зокрема, з ліва ні право зображені: екран запуску/зупинки збору даних з сенсорів; екран керування проведенням сесій збору даних та композитними активностями; екран вибору базових активностей; екран вибору суб'єкта збору даних; екран, що відображає інформацію про сенсори.

Рисунок 1 – Екрани розробленої програми для смарт-годинника

Дані збирають з триосьового акселерометра (з відкиданням гравітаційного прискорення) і гіроскопа з частотою дискретизації 100 Гц без видалення шуму. Ці дані допомагають відстежувати як зміну положення об'єкта у просторі, так і його орієнтацію. Структура даних з акселерометра та гіроскопа:

– акселерометр вимірює лінійне прискорення вздовж трьох осей (X, Y, Z). Дані включають: прискорення (м/с² або g) по кожній з осей; може вимірювати як силу земного тяжіння, так і прискорення від руху.

– гіроскоп вимірює кутову швидкість обертання навколо трьох осей (X, Y, Z). Дані включають кутову швидкість (градус/сек або рад/сек) по кожній осі.

Отримані дані передаються у вигляді кадру, що містить 3-секундний сигнал, записаний для певного каналу, разом з додатковими даними про тип основної діяльності, об'єкта, для якого збираються дані, позначку часу початку і закінчення сигналу, положення годинника (ліве або праве зап'ястя), частоту дискретизації і тривалість фрагмента сигналу. Кадри поміщаються в чергу і асинхронно передаються в хмарну базу даних по виділеному потоку. При втраті з'єднання або припиненні збору даних неповний кадр (тобто кадр, що містить запис сигналу тривалістю менше 3 секунд) відкидається і

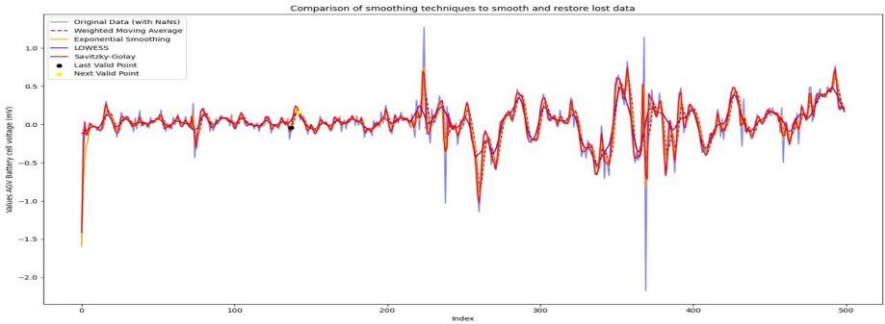
не відправляється в хмару. При формуванні набору даних кадр з однаковою початковою часовою міткою був об'єднаний в 1 6-канальний сигнал. Якщо 1 або більше каналів було втрачено, неповна група була відкинута.

Вплив втрати даних на точність роботи систем:

– акселерометри – втрата даних може призвести до помилок у визначенні положення або швидкості об'єкта. Оскільки акселерометр вимірює зміну швидкості, пропущені дані можуть негативно вплинути на точність розрахунків траєкторії та кутів нахилу.

– гіроскопи – втрата даних впливає на точність розрахунку орієнтації та кутового положення об'єкта. Оскільки гіроскопи вимірюють кутову швидкість, втрачені дані можуть призвести до накопичення помилок у визначенні орієнтації (дрейф гіроскопа).

Втрата даних із сенсорів у системі керування може спричинити неправильний аналіз рухів працівника, помилкових дій автоматизованих пристроїв або зниження загальної ефективності виробничих процесів. Для мінімізації впливу частково втрачених та спотворених даних використовуються методи імпутації, інтерполяції, фільтрації та згладжування. Фільтри допомагають згладити шум і компенсувати пропуски. Методи згладжування ефективно використовують для відновлення спотворених та частково втрачених даних на основі сусідніх значень. На рисунку 2 представлено результати доповнення частково втрачених даних за допомогою фільтрів: ковзного середнього, зваженого ковзного середнього, експоненційного згладжування, локальної регресії та фільтру Савіцького-Голея.



Відхилення	*Orig. Data*	*MA*	*WMA*	*ES*	*LO-WESS*	*SG*	*Дисперсія*	*Orig. Data*	*MA*	*WMA*	*ES*	*LO-WESS*	*SG*
X, axe	0.2824	0.2021	0.2086	0.2291	0.1795	0.2477	X, axe	0.0798	0.0408	0.0435	0.0525	0.0322	0.0613
Y, axe	0.5635	0.4323	0.4472	0.4618	0.4284	0.5160	Y, axe	0.3175	0.1869	0.2000	0.2133	0.1835	0.2662
Z, axe	1.0584	0.5361	0.5248	1.1328	0.4430	0.9993	Z, axe	1.1203	0.2874	0.2754	1.2832	0.1962	0.9987
X, hyr	0.2244	0.2040	0.2073	0.2074	0.2143	0.2225	X, hyr	0.0504	0.0416	0.0430	0.0430	0.0459	0.0495
Y, hyr	0.1189	0.1076	0.1103	0.1095	0.1130	0.1182	Y, hyr	0.0141	0.0116	0.0122	0.0120	0.0128	0.0140
Z, hyr	0.1962	0.1929	0.1934	0.1897	0.1913	0.1964	Z, hyr	0.0385	0.0372	0.0374	0.0360	0.0366	0.0386

Рисунок 2 – Порівняння методів відновлення даних

Ковзне середнє усереднює значення в певному вікні даних. Його легко реалізувати і він ефективно знижує рівень шуму в даних, які незначно змінюються з плином часу. Однак ковзне середнє не справляється з раптовими змінами в даних і може із затримкою реагувати на зміни фактичних даних. Зважене ковзне середнє більш чутливе до останніх змін, оскільки надає вагу новим даним. Воно може швидко реагувати на останні зміни, які корисні в динамічних умовах, але неправильно підібрані ваги роблять його занадто чутливим до короткострокових аномалій через неправильну інтерпретацію тенденцій або неправильних прогнозів. Експоненційне згладжування підвищує значимість останніх спостережень за рахунок експоненціального зменшення значущості старих даних. Воно добре підходить для систем, які потребують швидкої реакції на динаміку. Оскільки розрахунки виконуються поетапно і метод надає результати, які менш схильні до раптових коливань. Однак неправильно підібрані коефіцієнти можуть призвести до занадто повільної або занадто чутливої реакції.

Локальна регресія використовується для згладжування даних шляхом побудови локальної поліноміальної регресії з малими інтервалами між даними. Вона ефективно обробляє нелінійні дані, регулюючи ступінь полінома в кожному інтервалі, локально адаптуючи його до форми тренду в кожному інтервалі. Але для цього потрібна достатня кількість даних в кожному інтервалі. Фільтр Савіцького-Голея використовує локальну поліноміальну регресію для згладжування шуму в даних при збереженні піків і варіацій. Проте можна ефективно налаштувати степінь полінома та розмір вікна, щоб адаптувати його до різних типів даних та рівнів шуму. Але для згладжування без втрати інформації потрібна значна кількість даних. Якщо обраний розширений поліном, для розрахунку будуть потрібні значні ресурси. У цьому дослідженні з 5 методів згладжування і відновлення даних акселерометра і гіроскопа, отриманих за допомогою смарт-годинника Samsung Galaxy 5, локальна регресія дала найбільш точні результати.

Висновоки. Запропоноване в даній роботі використання даних з сенсорів смарт-годинників є значним покращенням, оскільки персонал повинен переміщатися по виробничому приміщенні у різних точках і при цьому виконувати декілька допоміжних дій. Наш підхід ґрунтується на використанні смарт-годинників для аналізу дій виробничого персоналу. Цей підхід дозволяє використовувати пристрої, перевірені для використання у спортивному тренуванні, і в той же час, завдяки їх популярності, є відносно недорогим рішенням. Розроблена аплікація дозволяє збирати дані триосьових акселерометра та гіроскопа із 3 секундною дискретністю із частостотою 100 Гц. Частково втрачені дані доцільно відновлювати локальною регресією. У подальших дослідженнях буде застосовано фільтр Калмана та розроблено нейромережну систему РЛД.

Інформаційні джерела

1. Li H., Shrestha A., Heidari H., Le Kernec J., & Fioranelli F. Bi-LSTM Network for Multimodal Continuous Human Activity Recognition and Fall Detection", IEEE Sensors Journal, вип. 20, вип. 3, pp. 1191–1201, Лют. 2020. doi: 10.1109/JSEN.2019.2946095.

2. Hussein R., Palangi H., Ward R., & Wang Z. J. Epileptic Seizure Detection: A Deep Learning Approach", 26, Березень 2018, arXiv: arXiv:1803.09848. doi: 10.48550/arXiv.1803.09848.

3. Butt F. S., La Blunda L., Wagner M. F., Schäfer J., Medina-Bulo I., & Gómez-Ullate D. Fall Detection from Electrocardiogram (ECG) Signals and Classification by Deep Transfer Learning", Information, вип. 12, вип. 2, Art. вип. 2, Лют. 2021. doi: 10.3390/info12020063.

4. Tzallas A. T., Tsipouras M. G., & Fotiadis D. I. Epileptic Seizure Detection in EEGs Using Time–Frequency Analysis, IEEE Transactions on Information Technology in Biomedicine, вип. 13, вип. 5, pp. 703–710, Вер 2009. doi: 10.1109/TITB.2009.2017939.

5. Dhiman C. & Vishwakarma D. K. A review of state-of-the-art techniques for abnormal human activity recognition", Engineering Applications of Artificial Intelligence, вип. 77, pp. 21–45, Січ. 2019. doi: 10.1016/j.engappai.2018.08.014.

6. Zhuang Z. і Xue Y., "Sport-Related Human Activity Detection and Recognition Using a Smartwatch", Sensors, вип. 19, вип. 22, Art. вип. 22, Січ. 2019. doi: 10.3390/s19225001.

7. Kalpesh J., Rushikesh J., Swaraj K., Rohan K., & Bharadwaj R. "Human Physical Activities Based Calorie Burn Calculator Using LSTM", Intelligent Cyber Physical Systems and Internet of Things, J. Hemanth, D. Pelusi, & J. I.-Z. Chen, Ред., Cham: Springer International Publishing, 2023, pp. 405–424. doi: 10.1007/978-3-031-18497-0_31.

8. Castro-García J. A., Molina-Cantero A. J., Gómez-González I. M., Lafuente-Arroyo S., & Merino-Monge M. Towards Human Stress and Activity Recognition: A Review and a First Approach Based on Low-Cost Wearables, Electronics, вип. 11, вип. 1, Art. вип. 1, Січ. 2022. doi: 10.3390/electronics11010155.

9. Ahmad Jalal, Majid Ali Khan Quaid, Sheikh Badar ud din Tahir, & Kibum Kim. A Study of Accelerometer and Gyroscope Measurements in Physical Life-Log Activities Detection Systems Sensors 2020, 20(22), 6670. URL: https://doi.org/10.3390/s20226670.

УДК 004.6

АНАЛІЗ І ВДОСКОНАЛЕННЯ МОДЕЛІ КЛАСТЕРИЗАЦІЇ ДАНИХ ДЛЯ ФОРМУВАННЯ ВИБІРКИ З МЕТОЮ ПРОГНОЗУВАННЯ РИЗИКОВИХ СИТУАЦІЙ

Орест ШОПСЬКИЙ
Ігор МАЛЕЦЬ

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The study presents the process of spell-checking, analyzes common spelling and grammatical errors, and identifies specialized abbreviations in large text data sets.*

Keywords: *linguistic model, large text data sets, operational-dispatch control, parallel processing, process optimization, specialized abbreviations, data clustering.*

Анотація. *У роботі представлено процес перевірки орфографії, здійснено аналіз типових орфографічних і граматичних помилок, а також виділено спеціалізовані абревіатури в великих масивах текстових даних.*

Ключові слова: *лінгвістична модель, великі блоки текстових даних, оперативно-диспетчерське управління, паралельна обробка, оптимізація процесів, спеціалізовані абревіатури, кластеризація даних.*

В роботах [1–3] неодноразово наголошувалось на необхідності очищення текстових даних від орфографічних помилок в описах подій, збережених в системі оперативно-диспетчерського управління. Це здійснюється з метою підвищення ефективності формування кластерів даних для розробки моделі штучного інтелекту, спрямованої на прогнозування ризикових ситуацій.

Критично важливим фактором при опрацюванні великих масивів даних є раціональне використання обчислювальних потужностей. В процесі проведення експерименту було реалізовано кілька практичних способів перевірки та підвищення ефективності опрацювання текстових даних. Ціллю цієї праці є представлення результату проведеної роботи, які стосуються аналізу типових помилок і виокремлення спеціалізованих абревіатур та назв у текстах описів подій.

Фрагментація опрацьовуваних записів

Одним і перших викликів при опрацюванні великих масивів текстових даних є часоємкий процес послідовного опрацювання кожного окремого запису. Внаслідок проведених експериментів опрацювання ~450000 записів займало ~8 днів. З іншого боку паралельне опрацювання усіх записів одночасно вимагало нереалістичних обчислювальних потужностей. Таким чином, вирішення цих проблем полягало передусім у пошуку оптимальної кількості одночасно опрацьовуваних записів. Враховуючи параметри наявних обчислювальних потужностей гіпотетичною кількістю оптимальної фрагментації даних є відповідність кількості блоків записів до кількості блоків ядер центрального процесора: 450000 : 60 = 7500. При проведенні практичного експерименту, моніторинг процесу виявив неоптимальне використання обчислювальних потужностей: при паралельному запуску процесів перевірки орфографії спочатку задіюється передусім жорсткий диск, при відносно вільних ресурсах центрального процесора, відтак, більшого навантаження зазнає процесор, при відносно вільному завантаженні жорсткого диску. Такий фактичний стан наштовхнув на ідею використання нерівномірного поділу записів по блоках, що при практичцій перевірці виявило позитивний результат. Проходження паралелізованої перевірки з нерівномірним поділом записів по блоках займає приблизно 12 хвилин.

Виклики формалізації типових помилок при навчанні NLP (Natural language processing) – моделі.

Оптимізація процесу опрацювання даних записів дала можливість швидше проходити кожну ітерацію виявлення наявних орфографічних та граматичних помилок з метою їх подальшого усунення. Слід зауважити, що суттєва частина їх насправді виявилась спеціалізованими визначеннями та абревіатурами таких як: КГП (керівник гасіння пожежі), АРЧ (аварійно-рятувальна час-

тина), ЗІЗОД (засоби індивідуального захисту органів дихання) і так далі. Природним чином відсутніми у використовуваному нами ВЕСУМ (Великий електронний словник української мови) [4, 5] та LanguageTool [6]. Додавання значень цих визначень та абревіатур у ВЕСУМ [4, 5] дозволить вважати їх частиною нормативного спеціалізованого словника.

Ще одним викликом оптимізації опрацювання даних є визначення та кластеризація типових помилок у описах подій бази даних системи оперативно-диспетчерського управління, таких як “караула”, “виїжали”, ”лейтинант” та інші. Створена таким чином база типових помилок допоможе у швидкому їх виявленні та виправленні у наявних та майбутніх записах бази даних СОДУ.

Висновки. У проведеному дослідженні було проаналізовано виклики та реалізовано практичні підходи до оптимізації обробки великих масивів текстових даних у системі оперативно-диспетчерського управління. Досягнуто суттєвого скорочення часу перевірки текстів шляхом впровадження нерівномірного розподілу записів на блоки для паралельного опрацювання текстової інформації. Виявлено, що значна частина “помилок” є спеціалізованими термінами та абревіатурами, які потребують додавання їх до словників інструментів перевірки. Додавання цих термінів у спеціалізований словник дозволяє підвищити точність аналізу та уникнути помилкового визначення цих термінів як орфографічних помилок. Формалізація та кластеризація типових помилок у записах бази даних СОДУ дала змогу створити базу помилок, яка може бути використана для подальшого навчання NLP-моделей. Це забезпечує можливість автоматизованого виявлення та виправлення помилок як у вже наявних, так і у нових записах. Отримані результати підвищують ефективність кластеризації даних для прогнозування ризикових ситуацій.

Інформаційні джерела

1. Martyn Ye., Smotr O., Burak N., Prydatko O., Malets I. Software for Shelter’s Fire Safety and Comfort Levels Evaluation. Communications in Computer and Information Science, Springer, Cham. – Vol. 1158, 2020, pp. 457–469. URL: https://doi.org/10.1007/978-3-030-61656-4_31.

2. Шопський О. М., Придатко О. В. Модель кластеризації даних для формування вибірки з метою прогнозування ризикових ситуацій. Збірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів 30.11.2023. – Львів, ЛДУ БЖД, 2023. – С. 466–468.

3. Шопський О. М., Придатко О. В., Малець І. О. Аналітика великих масивів даних для прогнозування ризикових ситуацій. Проблеми використання інформаційних технологій в освіті, науці та промисловості : матеріали 16 Міжнародної конференції 15.12.2021. – Дніпро, НУ “ДП”, 2021. – С. 212–214.

4. Старко В. Ф., Андрій Рисін. Великий електронний словник української мови (весум) як засіб NLP для української мови // Галактика Слова. Галині Макарівні Гнатюк / Ін-т укр. мови НАН України. – К. : Вид. дім Дмитра Бураго, 2020. – С. 135–141.

5. Великий електронний словник української мови. URL: https://github.com/brown-uk/dict_uk

6. LanguageTool. URL: https://languagetool.org/uk

УДК 004.424

АРХІТЕКТУРНІ ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ПРОГРАМНИХ СЕРВІСІВ З ПАРАЛЕЛЬНИМИ ОБЧИСЛЕННЯМИ

Іван РОВЕЦЬКИЙ

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The appearance of multi-core computing processors has made it possible to perform tasks in parallel (parallel computing). Using threads makes it possible to execute tasks in parallel. But there are often cases in practice when the performance of the service might be reduced. This is related to the specifics of creating, maintaining and managing threads. The architectural features of designing software services with parallel computing is analyzed in this paper.*

Keywords: *threads, thread pools, synchronization, parallel algorithms.*

Анотація. *З появою багатоядерних обчислювальних процесорів з'явилась можливість виконувати задачі паралельно (виконувати паралельні обчислення). Використання потоків дає можливість виконувати задачі паралельно, однак, на практиці дуже часто бувають випадки, коли відбувається погіршення продуктивності сервісу у багатопоточному середовищі. Це зумовлено, зокрема, особливостями роботи з потоками – створення, підтримки та керування потоками. У даній роботі проаналізовано архітектурні особливості проектування програмних сервісів з ефективним використанням потоків для виконання паралельних обчислень.*

Ключові слова: *потоки, пули потоків, синхронізація, паралельні обчислення.*

На даний час, існує два основних архітектурних рішення для проектування сервісів з паралельними обчисленнями: синхронний та асинхронний (реактивний).

Синхронна архітектура є класичним підходом, коли для паралельного опрацювання кожного клієнтського запиту виділяється окремий потік. Так працюють класичні веб-сервери Ця архітектура працює доволі добре і дає можливість масштабувати сервіс в залежності від навантаження, збільшуючи або зменшуючи кількість потоків у сервісі.

Створення потоку поєднує у собі не тільки створення певного об'єкту у адресному просторі процесу (*user space*), але це також додатковий виклик низькорівневого *API*-операційної системи з подальшим виконанням команд в адресному просторі ядра (*kernel space*), з допомогою яких відбувається резервування та ініціалізація певної кількість апаратних ресурсів, необхідних, зокрема, для зберігання стеку даних потоку, а також планування виконання необхідних інструкцій. Зрозуміло, що все це відбувається не миттєво і займає певний час, який стає особливо помітним у програмній системі під навантаженням.

Для уникнення негативного впливу динамічного створення потоків під час роботи сервісу, потрібно створювати деяку оптимальну кількість потоків одразу під час запуску програмного сервісу та перевикористовувати їх під час роботи програми. Для ефективного перевикористання потоків їх додають в пул. Оптимальну кількість потоків можна визначити тільки експериментально під час навантажувального тестування системи (*performance testing*).

Окрім резервування додаткової оперативної пам'яті, потоку потрібно як мінімум одне процесорне ядро для виконання запланованих програмних інструкцій. Звичайно, можна створювати більшу кількість потоків, аніж кількість процесорних ядер, однак, зрозуміло, що у цьому випадку у системі відбуватиметься не паралельний режим роботи, а так званий "конкурентний" режим роботи, який в цілому буде негативно впливати на продуктивність сервісу. Збільшення кількості потоків є доцільним тільки у випадку, коли в програмній системі існують блокуючі операції, такі як, *наприклад*, робота з файловою системою або базою даних, коли більшість потоків тривалий час перебувають у заблокованому стані і не сильно завантажують ядра процесора. У випадку, коли потрібно виконати складну і довготривалу обчислювальну задачу, створювати більше потоків, аніж кількість процесорних ядер, є недоцільно, оскільки це спричинить зайві втрати продуктивності на перемикання між потоками, а кількість виконаних корисних інструкцій залишиться тією ж самою.

Для того, щоб покращити продуктивність виконання довготривалих обчислювальних задач, використовують різноманітні паралельні алгоритми, а саме задачу розділяють на декілька незалежних підзадач, які виконують паралельно, а потім результати об'єднують. У випадку, якщо при цьому, використовуються запити до зовнішніх сервісів або баз даних, використовують неблокуючий інтерфейс (*асинхронний API*), якщо такий надається цими сервісами або базами даних. Це дає можливість паралельно запустити кілька задач, не блокуючи головний потік. Однак врешті решт все-таки доведеться дочекатися завершення роботи паралельних потоків, щоб отримати від них дані для подальшого об'єднання і повернення результату. Варто зауважити, що цей підхід можна застосувати тільки до певного класу задач, які володіють властивістю адитивності. В іншому випадку, якщо підзадачі залежать від порядку виконання, тоді розпаралелення може погіршити ситуацію, оскільки доводиться використовувати синхронізацію (блокування) потоків, що негативно впливає на продуктивність сервісу, тому задачі такого класу краще виконувати в одному потоці.

Використовуючи пули потоків та розпаралелення задач, можна покращити відгук системи, однак синхронний сервіс використовує блокуючі сокети для встановлення клієнтських з'єднань, тому такий сервіс не зможе прийняти більшу кількість запитів, ніж кількість вільних потоків у системі, оскільки кожен потік, який отримав клієнтський запит, блокуватиметься, доки не поверне результат. Щоб уникнути цього обмеження розроблено асинхронну архітектуру. В цій архітектурі існує тільки один головний потік (*EVENT LOOP*),

який приймає всі клієнтські запити та віддає відповідь асинхронно, використовуючи неблокуючі сокети (*NIO*). Опрацювання запитів відбувається в допоміжному пулі потоків, який, на відміну від синхронної архітектури, завжди має використовувати асинхронний *API*, щоб не блокувати головний потік. В протилежному випадку робота сервісу може просто зупинитись.

Висновки. Отже, у результаті проведеного дослідження встановлено, що особливістю сервісів з паралельними обчисленнями є ефективне використання потоків для виконання паралельних задач. Існують дві основні архітектурні моделі для створення сервісів з паралельними обчисленнями – синхронна та асинхронна. Можна використовувати як одну, так іншу, в залежності від класу задач. Синхронна модель показує хорошу продуктивність, однак має обмеження, пов'язані з блокуванням потоків, доки не буде отримано результати клієнтських запитів. Асинхронна модель дає можливість прийняти більшу кількість запитів, на відміну від синхронної, однак вимагає повністю асинхронного *API* під час роботи із зовнішніми сервісами, а також є складнішою під час відлагодження сервісу та виправлення помилок.

Інформаційні джерела

1. Goetz B. Java Concurrency in Practice / J. Bloch, T. Peierls, J. Bowbeer, D. Holmes, D. Lea. – 2010, 424 p.

2. Martin R. Clean Code: A Handbook of Agile Software Craftsmanship. – 2008, 464 p.

УДК 004.658

СИСТЕМА АНАЛІЗУ ДАНИХ ДЛЯ КУРСУ "МОДЕЛІ СТАТИСТИЧНОГО НАВЧАННЯ"

Богдан МАЛЕЦЬ
Тарас ЗАБОЛОЦЬКИЙ
Львівський національний університет імені Івана Франка, м. Львів, Україна.

Abstract. *The key aspects of the course "Statistical Learning Models" are analyzed with an emphasis on data generation, model building and their optimization. Data generation methods for various tasks are described: regression, classification models and time series models. The main types of statistical models are analyzed: regression, classification, clustering and models for working with time series, and examples of their practical application are also provided. Special attention is paid to the creation of synthetic data sets to test the stability and efficiency of models.*

Keywords: *data generation, statistical learning, regression, classification, clustering, time series, machine learning models.*

Анотація. *Проаналізовано ключові аспекти курсу "Моделі статистичного навчання" з акцентом на генерацію даних, побудову моделей та їхню оптимізацію. Описано методи генерації даних для різних завдань: регресійних, класифікаційних моделей і моделей часових рядів. Проаналізовано основні типи статистичних моделей: регресійні, класифікаційні, кластеризаційні та моделі для роботи з часовими рядами, а також надано приклади їх практичного застосування. Особливу увагу приділено створенню синтетичних наборів даних для перевірки стійкості та ефективності моделей.*

Ключові слова*: генерація даних, статистичне навчання, регресія, класифікація, кластеризація, часові ряди, моделі машинного навчання.*

Аналіз даних є основою багатьох сучасних технологій і рішень. У курсі "Моделі статистичного навчання" студенти вивчають, як будувати моделі, що дозволяють аналізувати великі обсяги даних, знаходити закономірності й робити прогнози. Ефективна система аналізу даних включає кілька ключових компонентів: підготовку та генерацію даних, вибір і навчання моделей, а також оцінку результатів і оптимізацію.

Генерація даних

Генерація даних є важливим етапом для розробки й тестування моделей. Вибір принципу генерації даних залежить від типу задачі та моделі, яку ви плануєте використовувати.

1. Генерація даних для регресійних моделей

Для задач регресії дані часто генеруються з урахуванням лінійних або нелінійних взаємозв'язків між змінними. *Наприклад*, можна створити синтетичний набір даних на основі рівняння:

$$y = 3x_1 - 2x_2 + \epsilon$$

де є – випадкова величина, що додає шум до даних (*наприклад*, з нормального розподілу). Це дозволяє симулювати реальні сценарії, коли значення залежної змінної залежить від кількох факторів, але містить похибки.

2. Генерація даних для класифікаційних моделей

Для задач класифікації використовуються методи, що створюють кластеризовані набори даних. *Наприклад*, можна генерувати точки, які належать до двох або більше класів у просторі, розділених певними межами. Популярний підхід – використовувати багатовимірний нормальний розподіл для кожного класу з різними центрами кластерів.

3. Генерація даних для моделей часових рядів

У задачах, де аналізуються часові ряди, дані можуть бути синтезовані на основі автокореляційних моделей або інших підходів. *Наприклад*, можна згенерувати набір, де значення на поточному кроці залежить від попередніх:

$$x_\tau = 0.8x_{\tau-1} + \epsilon_\tau$$

Це імітує поведінку реальних часових процесів, таких як ціни на ринку або зміни температури.

Моделі статистичного навчання

В основі аналізу даних лежать моделі статистичного навчання, які поділяються на кілька категорій залежно від їх мети:

1. Регресійні моделі

Регресія використовується для прогнозування числових значень. Основні методи включають лінійну регресію, регресію на основі регуляризації (Lasso, Ridge), а також нелінійні підходи, такі як поліноміальна регресія.

Приклад: Модель лінійної регресії використовує метод найменших квадратів для знаходження найкращої відповідності між змінними. Дані для таких моделей часто генеруються з урахуванням шуми, щоб перевірити їхню стійкість.

2. Класифікаційні моделі

Класифікація застосовується для прогнозування категорій (класів). Сюди входять моделі, такі як логістична регресія, метод опорних векторів (SVM), дерева рішень і ансамблеві методи (Random Forest, Gradient Boosting).

Приклад: Для класифікаційних моделей можна згенерувати набір даних, що імітує розділення класів у просторі, щоб перевірити, як модель справляється зі складними межами між ними.

3. Моделі кластеризації

Кластеризація – це метод поділу даних на групи на основі схожості. Популярні підходи включають K-means, DBSCAN та ієрархічну кластеризацію.

Приклад: Для кластеризації можна згенерувати точки, які групуються навколо кількох центрів у багатовимірному просторі.

4. Моделі для роботи з часовими рядами

Моделі, такі як ARIMA, LSTM, або Prophet, використовуються для аналізу даних, що змінюються з часом.

Приклад: Генерація синтетичних часових рядів із періодичними коливаннями й випадковим шумом дозволяє перевірити здатність моделі прогнозувати майбутні значення.

Інформаційні джерела

1. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning. Springer.

2. Kuhn M., Johnson K. Applied Predictive Modeling. Springer.

3. James G., Witten D., Hastie T., Tibshirani R. An Introduction to Statistical Learning. Springer.

4. Provost F., Fawcett T. Data Science for Business. O'Reilly Media.

УДК 614.84:004.9

ОНЛАЙН-СЕРВІС ДЛЯ ОПЕРАТИВНОГО РОЗРАХУНКУ СИЛ ТА ЗАСОБІВ ПОЖЕЖНО-РЯТУВАЛЬНИХ СЛУЖБ У ЖИТЛОВИХ БУДИНКАХ ПІДВИЩЕНОЇ ПОВЕРХОВОСТІ

Володимир МОТУЛЬСЬКИЙ
Олександр ХЛЕВНОЙ
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The online system calculates fire-rescue resources needed for firefighting in high-rise buildings. It ensures precise management of rescue resources in emergencies, considering the specifics of high-rise facilities, thereby enhancing safety for residents and rescuers.*
Keywords: *fire-rescue forces, high-rise buildings, online service, operational calculation.*

Анотація. *Онлайн-система оперативно розраховує сили та засоби пожежно-рятувальних служб для гасіння пожеж у багатоповерхових будинках. Вона забезпечує точне управління рятувальними ресурсами в надзвичайних ситуаціях, враховуючи специфіку висотних об'єктів, що підвищує безпеку мешканців та рятувальників.*
Ключові слова: *пожежно-рятувальні сили, багатоповерхові будівлі, онлайн-сервіс, оперативний розрахунок.*

Система розроблена для оперативного розрахунку рятувальних ресурсів, необхідних для безпечного та ефективного гасіння пожеж у висотних житлових будинках. Її мета – забезпечення швидкості та точності управління рятувальними ресурсами, враховуючи специфіку висотних об'єктів, що підвищує рівень безпеки для мешканців та рятувальників. Проблема пожежної безпеки житлових будівель ускладнюється зростанням щільності забудови та висотності будівель, що підвищує рівень пожежної небезпеки та ускладнює умови роботи пожежно-рятувальних служб. Згідно з Тимчасовим статутом дій у надзвичайних ситуаціях, головне завдання рятувальників – забезпечення порятунку людей та ліквідація пожежі в межах, які вона набуває на момент прибуття підрозділу [1]. Для успішного виконання цього завдання потрібна як висока теоретична підготовка, так і можливість оперативного доступу до актуальних даних щодо обстановки на об'єкті.

Онлайн-сервіс для оперативного розрахунку сил і засобів пожежно-рятувальних служб у висотних житлових будинках функціонує за багатоступеневим алгоритмом, що включає збір даних, розрахунки та планування ресурсів для ефективного реагування на пожежу. Система спершу збирає основні характеристики будівлі, такі як кількість поверхів, площа поверхів, відстань до пожежної частини, кут розповсюдження вогню, а також розта-

шування пожежних гідрантів, формуючи базу даних об'єкта і підготовлюючи дані для подальших розрахунків.

На першому етапі визначається час, протягом якого вогонь може вільно поширюватися до прибуття рятувальників. Це дозволяє оцінити масштаби пожежі на момент прибуття підрозділу. Далі, на основі часу вільного розвитку та параметрів об'єкта, система розраховує радіус поширення вогню за формулою:

$$R = 0{,}5 \cdot V_л \cdot \tau + V_л \, (\tau_{д.п.} - \tau),$$

де $V_л$ – лінійна швидкість поширення вогню, τ – час розгортання, $\tau_{д.п.}$ – час з моменту виникнення пожежі до початку подачі стволів. Обчислення радіуса поширення вогню допомагає визначити зону пожежного ураження, яка потребує першочергового втручання рятувальників.

Після визначення радіуса пожежі система розраховує площу, яка потребує гасіння, що дозволяє оцінити обсяг води та ресурсів, необхідних для припинення поширення вогню. Використовуючи розраховану площу гасіння, система визначає обсяг води, необхідний для локалізації пожежі. Загальна витрата води визначається за формулою:

$$Q_{заг}=Q_{гас}+Q_{зах},$$

де $Q_{гас}$ – витрата води на гасіння пожежі, $Q_{зах}$ – витрата на захист сусідніх поверхів та приміщень. Це враховує не лише витрати на гасіння пожежі, але й додаткові обсяги води для захисту конструкцій, які знаходяться поруч із вогнищем пожежі.

Система також оцінює, чи зможе перший підрозділ забезпечити достатній обсяг води для гасіння. Якщо ресурсів недостатньо, система планує залучення додаткових підрозділів, розраховуючи час їхнього прибуття. Крім цього, визначається необхідний обсяг води для захисту сусідніх конструкцій від пошкоджень та подальшого поширення вогню. Загальний обсяг витрати води підсумовується з урахуванням гасіння пожежі та захисних заходів.

На основі загального обсягу води система розраховує кількість пожежних автомобілів і особового складу, необхідних для забезпечення безперервної подачі води. При цьому враховується постійний тиск води та наявність додаткових водних ресурсів на об'єкті. Для підтримання належного тиску води також обчислюється гранична відстань від гідранта до будівлі, що дозволяє визначити, чи достатньо потужності наявного водопостачання для подачі води на висоту і площу.

Завершальний етап включає фінальне планування та забезпечення рятувальної операції необхідними ресурсами. Після всіх розрахунків система формує остаточний список необхідних сил і засобів: кількість пожежних автомобілів, особовий склад, та інші ресурси, необхідні для ефективного проведення пожежно-рятувальної операції у висотних житлових будинках. Цей комплексний підхід сприяє оперативному прийняттю рішень, що значно підвищує ефективність роботи рятувальників та безпеку мешканців у випадку пожежі.

Для підвищення ефективності роботи онлайн-системи та точності розрахунків доцільним є впровадження модулів для моніторингу реального часу та оновлення інформації про пожежу під час рятувальної операції. Це дозволить оперативно змінювати параметри розрахунку на основі фактичного розвитку пожежі, зокрема, розширювати зону ураження, розраховувати новий обсяг необхідних ресурсів та коригувати маршрут під'їзду додаткових підрозділів. Інтеграція з датчиками та системами раннього виявлення пожежі забезпечить автоматичне отримання первинних даних про займання, що ще більше підвищить точність і швидкість розрахунків. Використання алгоритмів штучного інтелекту дасть можливість аналізувати історичні дані пожеж у схожих будівлях для передбачення розвитку подій та налаштування плану рятувальних заходів. Автоматичне сповіщення мешканців та персоналу через SMS дозволить координувати евакуацію, вказуючи найбезпечніші виходи.

Висновки. Впровадження цієї онлайн-системи для багатоповерхових будинків забезпечує швидкий доступ до важливих тактико-технічних даних і дозволяє оперативно приймати рішення щодо розподілу сил і засобів для боротьби з пожежами. Система не лише підвищує ефективність рятувальних операцій, а й значно підвищує рівень безпеки у випадку пожеж у житлових висотних будинках, що є актуальним завданням для сучасних пожежно-рятувальних підрозділів.

Інформаційні джерела

1. Сировий В. В., Сенчихін Ю. М., Ушаков Л. В., Бабенко О. В. Аналітичні розрахунки для обґрунтування оперативних дій пожежно-рятувальних підрозділів: Практикум / НУЦЗУ. – Харків: НУЦЗУ, 2010. – 236 с.

2. Декальчук Р. Пожежна тактика та розрахунок сил і засобів / ВУЗ Цивільного Захисту України. – Київ: Видавництво, 2019. – 289 с.

3. Гуревич Р. С., Кадемія М. Ю., Шевченко Л. С. Інформаційні технології навчання: інноваційний підхід. – Вінниця: Планер, 2012. – 348 с.

УДК 004.056.5:005.8

СИСТЕМА БРОНЮВАННЯ ЖИТЛА ДЛЯ ВОЛОНТЕРІВ

Олег ЛИБА
Роман ГОЛОВАТИЙ

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Анотація. *A housing reservation system for volunteers is proposed that simplifies the search and reservation of apartments. Using the MVC architecture in Spring Boot allows us to build a scalable and efficient system that provides quick access to the necessary housing for volunteers.*

***Keywords**: apartment booking, volunteers, booking system, MVC architecture, Spring Boot, housing support, volunteer service, accommodation management, availability, residency organization.*

***Abstract.** Запропоновано систему бронювання житла для волонтерів, яка спрощує пошук і резервування квартир. Використання архітектури MVC у Spring Boot дозволяє побудувати масштабовану та ефективну систему, що забезпечує швидкий доступ до необхідного житла для волонтерів.*

***Ключові слова**: бронювання житла, волонтери, система бронювання, MVC-архітектура, Spring Boot, житлова підтримка, сервіс волонтерів, управління житлом, доступність, організація проживання.*

У сучасних умовах, коли волонтерська діяльність набирає значної популярності, пошук тимчасового житла для волонтерів є важливою та необхідною задачею. Забезпечення доступу до житла дозволяє волонтерам зосередитись на соціальних ініціативах, не витрачаючи зайвих ресурсів на пошук житлових умов. Розробка спеціальної системи бронювання житла для волонтерів, яка враховує їхні особливі потреби, сприятиме покращенню процесу організації волонтерської діяльності.

Система, побудована на Spring Boot з архітектурою MVC (рис. 1), забезпечує модульний підхід, що дозволяє спростити процес підтримки та розвитку платформи. Використання MVC-патерну дозволяє розділити логіку застосунку на три основні компоненти, що сприяє легшій організації коду та підвищенню ефективності роботи.

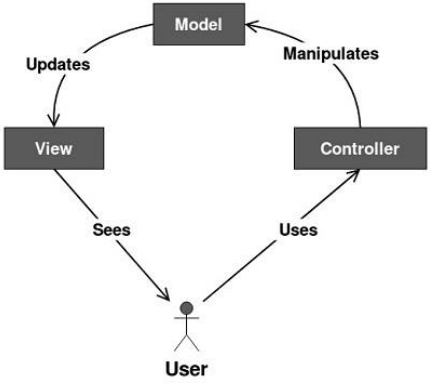


Рисунок 1 – Графічне представлення типової структури MVC архітектури

Існують численні комерційні системи для бронювання житла, такі як Airbnb [1] та Booking.com [2], які пропонують можливості з оренди та резервування житла для широкого кола користувачів. Проте ці платформи не завжди враховують специфічні потреби волонтерів, для яких важливими є

знижені ціни або можливість безкоштовного проживання. Система бронювання житла для волонтерів, побудована на основі архітектури MVC, здатна ефективно обробляти подібні запити, забезпечуючи волонтерам необхідні умови проживання.

Spring Boot є потужною платформою для розробки веб-додатків на Java, яка підтримує швидке створення застосунків з мінімальною кількістю налаштувань [3, 4]. Архітектура MVC, яка чітко розділяє компоненти на Model, View та Controller, дозволяє спростити розробку, тестування та подальше розширення системи. Це забезпечує модульність, масштабованість та підтримку ефективної взаємодії між частинами застосунку.

Model представляє дані та бізнес-логіку застосунку. У контексті системи бронювання житла для волонтерів модель включає такі сутності, як “Квартира”, “Волонтер”, “Бронювання”, “Доступність”. Кожна з цих сутностей відповідає за збереження конкретної інформації: “Квартира” містить деталі про розташування, доступність та характеристики житла; “Волонтер” зберігає інформацію про волонтера, що резервує житло; “Бронювання” контролює дані про підтверджені запити на житло. ORM (Object-Relational Mapping) у вигляді JPA дозволяє спрощено управляти цими даними та інтегрувати їх у базу даних для подальшого збереження і доступу.

Controller відповідає за обробку запитів користувача і скеровує їх до відповідних методів у сервісному рівні. *Наприклад*, “BookingController” та “ApartmentController” обробляють запити на перегляд доступних квартир, створення бронювань та їх скасування. Ці компоненти дозволяють волонтерам швидко знаходити та резервувати доступне житло відповідно до їхніх потреб, зручний інтерфейс для перегляду та оновлення бронювань.

Service виконує основну бізнес-логіку системи. Для системи бронювання житла “BookingService” забезпечує перевірку доступності квартир, обробку можливих конфліктів при бронюванні та актуалізацію розкладу бронювань. Такий поділ на окремий сервісний рівень полегшує тестування бізнес-логіки та знижує ймовірність виникнення помилок у контролерах. Додатково, сервісний рівень контролює відповідність даних перед їх записом до бази.

Висновки. Розробка системи бронювання житла для волонтерів на основі Spring Boot з використанням MVC-патерну дозволяє створити надійну та ефективну платформу, що забезпечує легкість використання, масштабованість та зручність для волонтерів. Система здатна відповідати на потреби організацій, що залучають волонтерів, полегшуючи процес пошуку житла та організацію волонтерської діяльності загалом.

Інформаційні джерела

1. Airbnb. Airbnb | Помешкання для відпустки, зруби, будинки на пляжі тощо. URL: https://www.airbnb. com.ua/.

2. Система інтернет-бронювання житла – Booking.com. URL: https:// booking.com.

3. Зачко О. Б., Головатий Р. Р. Мультиагентна модель управління безпекою при плануванні проектів створення об'єктів з масовим перебуванням людей. Стратегічне управління, управління портфелями, програмами та проектами. 2017. № 2 (1224). – С. 46–51.

4. Смотр О., Рашкевич О. М., Головатий Р., Мечус Х. Використання інструментарію інформаційних технологій для підвищення мотивації студента до навчання у форматі змішаної освіти. Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : Збірник наукових праць. Випуск 6. / За ред. М. С. Коваля, Н. Г. Ничкало. – Львів : ЛДУ БЖД, 2021. – С. 214–217.

УДК 004.4: 614.8

СТВОРЕННЯ ІНТЕГРОВАНОЇ МОБІЛЬНОЇ СИСТЕМИ ДЛЯ КООРДИНАЦІЇ ГУМАНІТАРНОЇ ДОПОМОГИ ТА ЕВАКУАЦІЙНИХ ЗАХОДІВ

Павло ПОГЛОД
Ольга СМОТР
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The theses substantiate the need for developing a mobile system to coordinate humanitarian aid and evacuation efforts for both civilian and military needs. Functional modules, methods of ensuring information security, integration with cloud services, and development prospects are presented. Key challenges related to system development and implementation are highlighted.*

Keywords: *mobile system, humanitarian aid, evacuation, military needs, Android Studio, information security.*

Анотація. *У роботі обґрунтовано необхідність розробки інтегрованої мобільної системи, яка дозволить координувати гуманітарну допомогу та евакуаційні заходи як для цивільних, так і для військових потреб. Представлено функціональні модулі, методи забезпечення інформаційної безпеки, інтеграцію з хмарними сервісами та перспективи розвитку. Зазначено ключові виклики, пов'язані з розробкою та впровадженням системи.*

Ключові слова: *мобільна система, гуманітарна допомога, евакуація, військові потреби, Android Studio, інформаційна безпека.*

Війна, яка триває в Україні, спричинила масштабну гуманітарну кризу, що вимагає швидкої мобілізації ресурсів для забезпечення як цивільних, так і військових потреб. До цих потреб належать доставка гуманітарної допомоги в постраждалі регіони, евакуація мирного населення, а також підтримка військових підрозділів з метою забезпечення їх критично важливими ресурсами.

У сучасних умовах, коли ресурси обмежені, а ситуація стрімко змінюється, критично важливою є задача створення системи, що могла б забезпечити ефективне управління логістикою, прозорість розподілу допомоги та своєчасне реагування на надзвичайні ситуації. Беручи до уваги, що це повинна бути система оперативного реагування, доступна кожному українцю, система, яка б могла бути завше під рукою та те, що більшість користувачів в Україні використовують для виходу в глобальну мережу смартфони [1], вважаємо, що найефективніше буде розробити таку систему у формі інтегрованого мобільного додатку. Пропонуємо розробити мобільну систему, що стане універсальним інструментом для координації цих процесів, використовуючи можливості сучасних цифрових технологій.

В результаті вивчення проблеми та базуючись на аналізі додатків аналогів [2–3] ми прийшли до висновку, що така система першочергово повинна вирішувати три таких ключових задачі:

– оперативний доступ до інформації про потреби в регіонах;

– прозорість у розподілі допомоги для цивільних і військових;

– надання точних даних для організації евакуацій.

Основні модулі системи відображено на рисунку 1.

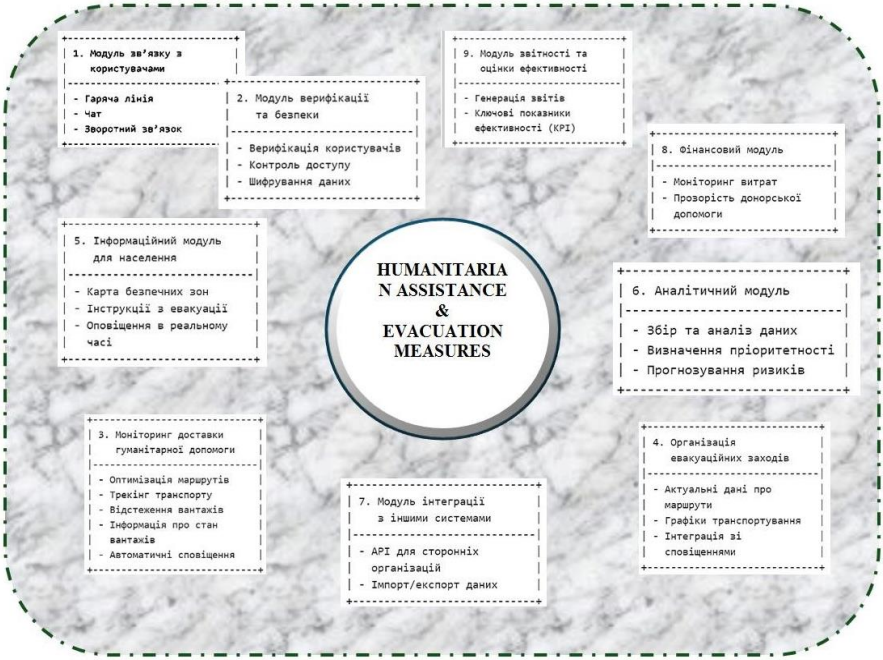


Рисунок 1 – Ключові модулі мобільної системи для забезпечення координації гуманітарної допомоги та евакуаційних заходів

Хочемо, зауважити, що не верифіковані користувачі матимуть доступ лише до інформаційного модуля до системи. Тобто доступ до карт з нанесеними безпечними для переміщення зонами (гуманітарними хабами) та доступ до інструктивних матеріалів, щодо першочергових дій, які необхідно знати для безпечної евакуації та інструктивних матеріалів щодо надання першої медичної допомоги.

Вважаємо за доцільне серед основних технологічних рішень, що використовуватимуться у проєкті закласти можливість використання хмарних сервісів та інтеграції з API: З метою забезпечення доступності та швидкої обробки запитів, доступу до картографічних даних, геолокації та інструментів моніторингу в реальному часі (рис. 2).

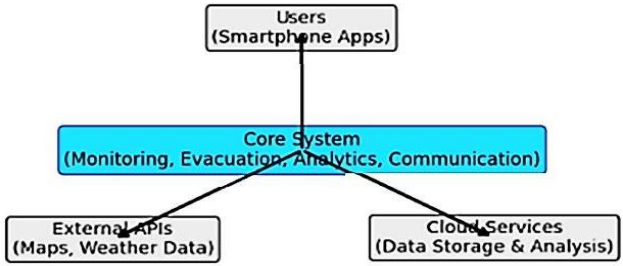


Рисунок 2 – Схема роботи мобільної системи

Основні виклики, що можуть виникнути при розробці даної системи можна розділити на три категорії:

– *Технічні виклики*: Забезпечення роботи системи у регіонах із низькою якістю зв'язку через механізми автономного функціонування.

– *Юридичні виклики*: Дотримання вимог міжнародного законодавства щодо обробки персональних даних.

– *Етичні виклики*: Баланс між потребами цивільного населення і військовими запитами.

Висновки. Розробка системи, що забезпечить ефективне управління процесами надання гуманітарної допомоги та евакуацій в кризових ситуаціях на сьогодні є нагальною потребою сьогодення. Її впровадження сприятиме підвищенню оперативності дій, прозорості процесів і ефективності координації між цивільним та військовим секторами. Доцільно розробити таку систему у формі інтегрованого мобільного додатку з використанням можливостей сучасних цифрових технологій: використання хмарних сервісів; інтеграція з API; інструментарій моніторингу даних в реальному часі тощо.

Інформаційні джерела

1. Електронний ресурс. URL: https://gemius.com/ua/%D0%B1%D0%BB%D0%BE%D0%B3/internet-and-media-in-ukraine-february2024-report/

2. Ініціатива Гарвардської гуманітарної допомоги. (2011). Допомога у надзвичайних ситуаціях 2.0: Майбутнє обміну інформацією в умовах гуманітарних криз. Технологічне партнерство Фонду ООН і Фонду Vodafone.

3. Меєр П. (2012). Цифрові гуманітарії: Як великі дані змінюють обличчя гуманітарної реакції. CRC Press.

4. Кордунова Ю., Смотр О., Кокотко І., & Малець Р. (2021). Аналіз традиційного та гнучкого підходів до створення програмного забезпечення в динамічних умовах. Управління розвитком складних систем, (47), С. 71–77. URL: https:// doi.org/ 10.32347/ 2412-9933.2021.47.71-77

5. Придатко О., Смотр О., Мартин Є., Придатко В. Оптимізація методів теорії масового обслуговування для вирішення прикладних завдань розвитку регіональних систем безпеки життєдіяльності. Системи обробки інформації. 2019. Вип. 2 – С. 146–152.

УДК 004.4: 614.8

РОЗРОБКА МОБІЛЬНОГО СЕРВІСУ НАДАННЯ ПСИХОЛОГІЧНОЇ ДОПОМОГИ

Віталій ГАПАНОВИЧ
Ольга СМОТР

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The article substantiates the need for a mobile application for psychological assistance, providing access to consultants in real time and offering interactive tools for self-help. Special attention is given to the use of the Unity platform for implementing game mechanics that enhance users' psychological well-being. The system's architecture, implementation challenges, and development prospects are discussed.*

Keywords: *psychological assistance, mobile application, interactivity, information security.*

Анотація*. У роботі обґрунтовано необхідність створення мобільного додатку надання психологічної допомоги, який забезпечує доступ до консультантів у реальному часі та пропонує інтерактивні інструменти для самодопомоги. Особливу увагу приділено важливості персоналізації даного сервісу, для користувача, що сприяриме покращенню психологічного стану користувачів. Розглянуто архітектуру системи, виклики у впровадженні та перспективи розвитку.*

Ключові слова*: психологічна допомога, мобільний додаток, інтерактивність, інформаційна безпека.*

Сучасний світ стикається з різким зростанням кількості людей, які потребують психологічної підтримки через стрес, депресію та кризові стани. На жаль, доступ до професійної допомоги залишається обмеженим через дефі-

цит спеціалістів, вартість послуг та географічні бар'єри. Для України, на сьогодні, питання надання психологічниї підтримки в умовах війни стоїть дуже гостро. Цей проєкт має на меті створення інтерактивного мобільного додатку, який забезпечить швидкий доступ до консультантів у реальному часі та запропонує ефективні інструменти для самодопомоги. Додаток має стати надійним і доступним ресурсом, який зменшить бар'єри до надання психологічної допомоги завдяки використанню сучасних технологій.

З метою створення ефективного продукту було проведено аналіз існуючих систем аналогів. Нами було досліджено такі системи, як BetterMe, VOS та DOOMKA. BetterMe пропонує курси для релаксації та подолання стресу, однак не включає функцій реального часу взаємодії з психологами. VOS дозволяє звертатися до коучів і психологів, але його інтерфейс не надто доступний, тож часто викликає труднощі у користувачів, щодо розуміння їх дій. DOOMKA надає прості вправи для зниження стресу, але не забезпечує персоналізованих рекомендацій і професійної підтримки. Враховуючи ці недоліки, було розроблено концепцію вдосконаленої системи, яка об'єднує сильні сторони досліджених застосунків та намагитеметься максимально нівілювати наведені недоліки.

Вважаємо, що доцільно розробити систему надання психологічної допомиги, що включатиме наступні такі компоненти:

– мобільний додаток (UI) – забезпечує інтуїтивний інтерфейс для взаємодії користувача із системою;

– сервер (Backend) – обробляє запити користувачів, керує доступом до ресурсів і виконує функції бізнес-логіки;

– база даних – забезпечує збереження інформації про користувачів, їхній прогрес і взаємодію із системою;

– модуль аналітики – аналізує дані користувачів для надання персоналізованих рекомендацій;

– модуль відео/аудіо зв'язку – реалізує можливість проведення сесій із психологами у реальному часі;

– модуль інтерактивних вправ – пропонує релаксаційні техніки, вправи для концентрації та подолання стресу;

– інтеграція із зовнішніми API – дозволяє використовувати технології штучного інтелекту та доповненої реальності для покращення взаємодії.

Пропонована структурна схема системи мобільного сервісу надання психологічної допомоги відображена на рисунку 1.

Основними перевагами пропонованої системи мобільного сервісу надння психологічної допомоги додатку вважаємо можливість контакту з консультантами в режимі реального часу в форматі відео- та аудіоконференцій. Окрім того, можливість обміну текстовими повідомленнями для користувачів, які віддають перевагу письмовій формі, у форматі чату для консультацій. Також у даній системі будуть доступними інтерактивні вправи, що сприяють зменшенню стресу та релаксації, для прикладу, візуалізація технік дихання.

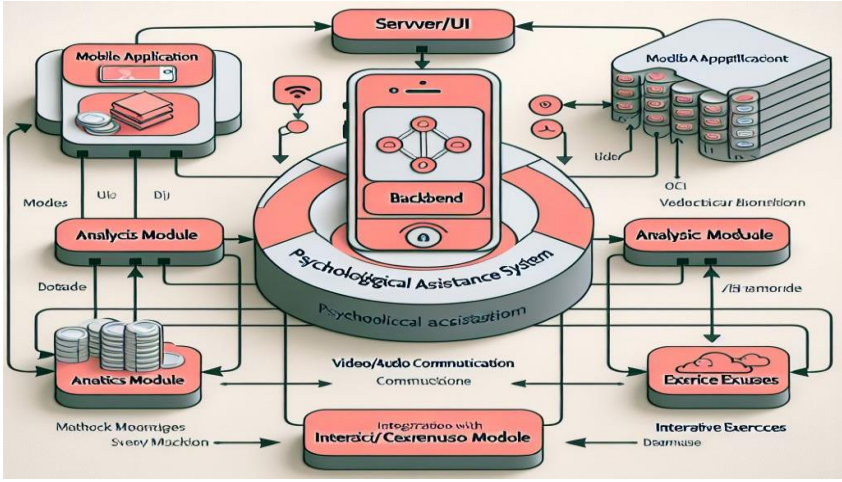


Рисунок 1 – Схема архітектури системи мобільного сервісу надння психологічної допомоги

Ще одним, важливим питанням, яке обовязково повиннобути забезчене при функціонуванні даного додатку, є питання гарантії конфіденційності: Адже психологічна допомога часто пов'язана з дуже чутливою інформацією, яка стосується емоційного стану, особистих проблем, стосунків чи травматичних подій. Тому мега важливим є створити безпечний простір для відкритого спілкування, що відповідав би етичним принципам психології, які вимагають захисту даних клієнтів та забезпечив довіру користувачів до додатка. З метою забезпечення конфіденційності варто передбачити:

– шифрування даних на всіх етапах (зберігання, передача);
– анонімізацію або псевдонімізацію інформації;
– використання систем багаторівневої аутентифікації для захисту акаунтів;
– чітку політику конфіденційності, доступну користувачам;
– регулярний аудити безпеки та тестування на проникнення.

Гарантуючи конфіденційність, мобільний додаток для психологічної допомоги сприятиме створенню безпечного середовища для користувачів, підвищуючи їхнє благополуччя та довіру до сервісу.

В майбутньому дану систему доречно було б доповнити модулями, що базуються на можливостях штучного інтелекту, А саме, розробити модулі для аналізу емоційного стану користувачів, створити віртуальне середовище для релаксації, з використанням інструментарію доповненої реальність (AR). Також на нашу думку значний позитивний ефект принесло б використання розробленого мобільного сервісу надння психологічної допомоги разом з постійним моніторингом здоров'я користувача. Тобто, інтеграція з носимими пристроями для розширення функціоналу.

Висновки. Розробка мобільного сервісу надання психологічної допомоги відкриває нові можливості для забезпечення доступності психологічної підтримки. Використання інтерактивних механік сприяє ефективнішій взаємодії з користувачами, підвищуючи їхню мотивацію та зручність у використанні сервісу.

Інформаційні джерела

1. Боуен Р. К., Боуен А. К. Додатки для підтримки психічного здоров'я: Використання цифрових інструментів для психологічної допомоги. Current Psychiatry Reports, 2021, 23(10). – С. 1–7.

2. Kordunova Y., Smotr O., Kokotko I., Malets R. Analysis of the traditional and flexible approaches to creating software in dynamic conditions. Manage. Dev. Complex Syst. pp. 71–77 (2021). URL: https://doi.org/10.32347/2412-9933.2021.47.71-77

3. Сміт А. Дж., Джонсон Т. Р. Інтерактивні методи зниження стресу за допомогою мобільних додатків. Journal of Medical Internet Research, 2020, 22(8), e17709.

4. Martyn Y., Smotr O., Burak N., Prydatko N. and Malets I. Informational graphic technologies for fire safety level determination in special purpose buildings, in: Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020, 2020, pp. 398–403. doi: 10.1109/DSMP47368.2020.9204180.

5. Кордунова Ю. С., Фелтіновскі М., Придатко О. В., Смотр О. О. Математичне моделювання процесу розробки спеціалізованих програмних систем безпекоорієнтованого спрямування. Вісник Львівського державного університету безпеки життєдіяльності. – Львів: Вип. 27, 2023. – С. 23–31. doi: 10.32447/ 20784643.27. 2023.03.

УДК 004.8:502.3:504.75

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СТВОРЕННЯ ПОРТАЛУ АВТОСПОРТИВНИХ НОВИН

Т. БЛИЗНЮК

Державний університет "Житомирська політехніка", м. Житомир, Україна.

Abstract. *The theses are devoted to the development of software for creating a specialized web portal of motorsports news. The choice of technologies, the architecture of the portal, and its functionality are described.*

Keywords: *motorsport, web portal, TypeScript, React, PostgreSQL, REST API, Docker, frontend, backend, scalability.*

Анотація. *Тези присвячені розробці програмного забезпечення для створення спеціалізованого веб-порталу автоспортивних новин. Описано вибір технологій, архітектура порталу, його функціональні можливості.*

Ключові слова: *автоспорт, веб-портал, TypeScript, React, PostgreSQL, REST API, Docker, frontend, backend, масштабованість.*

На сьогодні автоспорт є одним з найпопулярніших та найприбутковіших видів спорту, що поєднує в собі швидкість, небезпеку, витривалість, вир емоцій та насолоду від перемоги. Станом на 2024 рік Формула 1 налічує більш, ніж 500 млн. фанатів по всьому світу, також популярними є NASCAR, IndyCar, WEC, молодші серії F1, картинг тощо.

Враховуючи популярність та славу даного виду спорту, потрібно створити “місце” (далі – портал), де користувачі зможуть ділитися враженнями від перегляду різноманітних гонок, редактори порталу – додавати статті про новини в світі автоспорту, а адміністратори – контролювати якість контенту на порталі, додавати новий функціонал, аналізувати наявні дані та реагувати на скарги інших користувачів. Наявність нових технологій та бібліотек дозволяє реалізувати дане програмне забезпечення (далі – ПЗ).

Дане ПЗ має бути доступним для користувачів з будь-яких сучасних браузерів, підтримувати різноманітні девайси та отримувати інформацію в режимі реального часу. Також варто замислитися над іншими факторами: місцем зберігання даних (особливо фото- та відео-файлів) для ПЗ, різноманітними оптимізаціями, доступністю та масштабованістю ПЗ (для доступу в мережі Internet), а також захищеністю даних.

Після проведеного аналізу вирішено розділити ПЗ на 2 частини: backend (сервер, бізнес-логіка для запитів) та frontend (основа ПЗ, його вигляд в браузері). Backend-частина буде приймати від користувачів та віддавати користувачам дані для збереження та отримання, керувати правами доступу та оптимізаціями (такими, як кешування даних), а також мати запити для різноманітних дій. Натомість frontend-частина являє собою представлення самого вигляду ПЗ (в нашому випадку – сайт-портал) за допомогою розмітки на базі розмітки HTML, стилізації за допомогою каскадних стилів CSS та функціонування сторінок на базі мови програмування JavaScript (рис. 1).

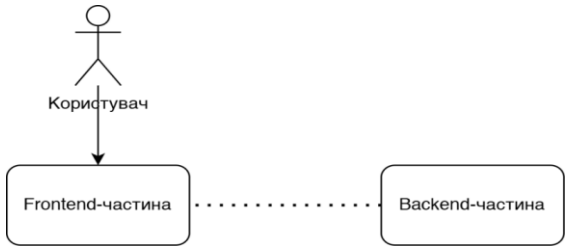


Рисунок 1 – Взаємодія між користувачем, frontend- та backend-частинами додатку

Backend-частина порталу – це серверний додаток на базі REST API. Якщо більш зрозуміліше, це поєднання посилань (HTTP-запитів) на запити та відповідні обробники (функції), які виконують ту чи іншу серверну логіку. До кожного посилання можна прив’язати свій обробник, який буде виконувати влас-

ний код. Ця частина ПЗ виконує різноманітні задачі: отримання даних з баз даних (далі – БД), занесення даних до БД, планування задач, зібрання інформації для аналітики тощо. Для написання backend-частини використовується мова TypeScript, яка є розширенням всіма відомого JavaScript. Також backend-частина буде керувати кешуванням – збереженням даних у легших БД задля швидшого отримання даних на frontend-частині.

У [0] представлено порівняльну характеристику систем управління реляційними базами даних PostgreSQL та MySQL, проведено їх детальний аналіз та опис, а також зіставлено їх для висвітлення переваг та недоліків кожної.

Для збереження даних порталу автоспортивних новин будуть використовуватися декілька систем збереження даних: реляційна система управління БД (далі – СУБД) PostgreSQL, побудована на стандарті SQL та відома своєю масштабованістю та надійністю – для збереження основних даних звичайних типів, сховище Firebase Storage від Google – для збереження фото- та відео-файлів та легкі БД типу "ключ-значення" – для збереження кешованих даних.

Автором [0] розглянуто основні аспекти розробки вебсайтів за допомогою HTML, PHP, JavaScript та CSS. Особлива увага приділена використанню цих технологій для створення ефективного та захоплюючого вебжурналу про екстремальні види спорту. У теоретичній частині дослідження детальному вивчаю теоретичних основ використання цих технологій, включаючи їх потенціал у контексті розробки вебжурналів.

Для порталу автоспортивних новин Frontend-частина – це веб-сайт, тобто те, що бачить користувач у браузері. Користувач отримує різноманітні дані, в тому числі й відображення сторінок (семантика HTML, стилі CSS та функціонал JavaScript) за допомогою протоколу HTTP-запитів. За тим же протоколом клієнт (тобто frontend-частина) отримує дані з backend-частини. Для створення frontend-додатку використовується бібліотека React, відома своєю простотою у використанні та створенні компонентів, які можна використовувати багаторазово без втрати продуктивності. Аналогічно до backend-частини, весь код на frontend-частині написаний на мові TypeScript.

Docker надає фреймворк для пакуваннядодатків та їх залежностей у контейнери, пропонуючи портативність, ізоляцію та ефективне використання ресурсів. Контейнери гарантують узгоджену роботу додатків у різних середовищах [0].

Після того, як обидві частини для порталу автоспортивних новин створені, можна приступити до процесу "деплою" (контейнеризації обох частин порталу задля розміщення на різноманітних хостингах). Для цього можна використати інструмент Docker, який дозволяє запускати додатки на "контейнерах" (окремих віртуальних машинах). Це суттєво допомагає з масштабованістю порталу для подальшого розміщення на хостингу.

Висновки. Отже, вище були подані кроки для створення порталу автоспортивних новин. І хоч його вже можливо назвати функціонуючим, але

на цьому його розробка не зупиняється. Є можливість розширювати наявний функціонал на обох сторонах поралу за потреби. Також за наявним backend-ом можливо створити мобільний додаток, який буде виконувати аналогічну роботу до frontend-застосунку. У перспективі портал може бути розширений за рахунок впровадження систем прогнозування результатів, інтеграції live-трансляцій та монетизації через платні підписки чи рекламу. Дана розробка є важливим кроком у розвитку цифрової інфраструктури автоспорту, а також підвищення обізнаності про даний вид спорту серед звичайних користувачів мережі Internet.

Інформаційні джерела

1. Маренко Д. В., and Бабюк Н. П. Розробка та наповнення бази даних програмного засобу для організації велоінфраструктури міста. Diss. Вінницький національний технічний університет, 2024.

2. Ковалевський М. М. Розробка інформаційної системи з використанням HTML, PHP, JavaScript, CSS : кваліфікаційна робота освітньо-професійного ступеня фаховий молодший бакалавр спеціальності 021 “Інженерія програмного забезпечення” освітньо-професійної програми “Розробка програмного забезпечення” / наук. керівник О. В. Чопорова. Запоріжжя : ВСП ЕПФК ЗНУ, 2024. 48 с.

3. Кутуєв Олександр. Алгоритм застосування інструменту docker для оптимізації розгортання та запуску веб-додатків. The 12 th International scientific and practical conference “European scientific congress” (December 25–27, 2023) Barca Academy Publishing, Madrid, Spain. 2023. 705 p.

УДК 004.5

ПАНЕЛЬ КЕРУВАННЯ ДЛЯ СИСТЕМИ РОЗУМНОГО БУДИНКУ НА БАЗІ ЧАТ-БОТУ МЕСЕНДЖЕРА

Зореслава ШПАК
Михайло ШУВАР
Національний Університет “Львівська політехніка”, м. Львів, Україна.

Abstract. *The advantages and disadvantages of using the Telegram messenger chatbot as a smart home control panel are considered. The architecture of an information messaging system based on the Arduino board and the Raspberry Pi microcontroller using an asynchronous data processing process is described.*

Keywords: *smart home, messenger, control panel, Arduino, Raspberry Pi.*

Анотація. *Розглянуто переваги та недоліки використання чат-бота месенджера Telegram як панелі керування розумним будинком. Описано архітектуру системи обміну інформаційними повідомленнями на базі плати Arduino і мікроконтролера Raspberry Pi із застосуванням асинхронного процесу опрацювання даних.*

Ключові слова: *розумний будинок, месенджер, Arduino, Raspberry Pi.*

Розумні будинки, що дають змогу ефективно використовувати різноманітні системи життєзабезпечення житла, стають щораз більше затребуваними у наш час [1]. Для зручності користувачів розробляються спеціальні застосунки і платформи дистанційного керування розумним будинком через мережу інтернет. Проте реалізація такого підходу здебільшого вимагає серверів комунікації, що може істотно впливати на загальну вартість системи і стає проблемою для бюджетних проєктів.

Рішенням цієї проблеми може бути використання вже наявних платформ. Однією з них є Telegram – один з найпоширеніших месенджерів у світі [2]. Перевагою цього месенджера є зручний інтерфейс, за допомогою якого можна легко створити панель керування. Крім цього, Telegram надає простий і функціональний API, що підтримується багатьма бібліотеками мови Python і уможливлює адаптивну реалізацію панелі керування в цьому месенджері.

Загальна схема опрацювання інформаційних повідомлень системи розумного будинку із застосуванням месенджера Telegram подана на рисунку 1.

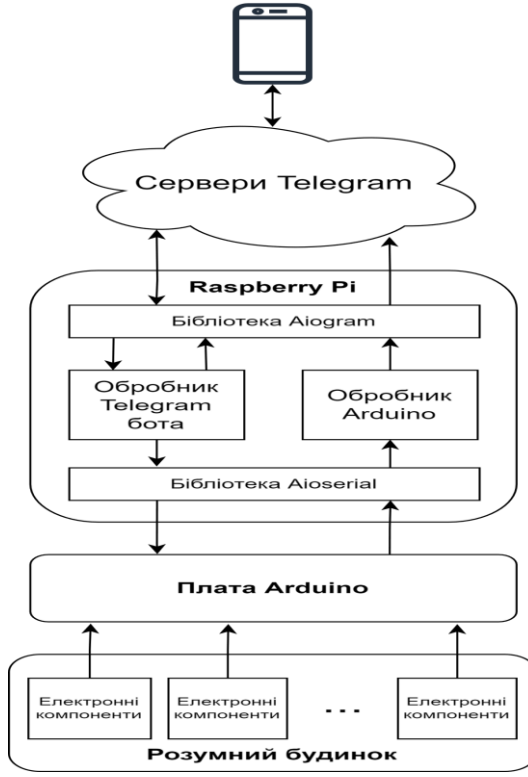


Рисунок 1 – Загальна схема системи обміну повідомленнями

Всі компоненти безпосереднього керування і взаємодії з виконавчими механізмами і приладами розумного будинку, давачі, контролери та інші елементи під'єднуються до входів або виходів плати Arduino. Мікроконтролер Arduino з'єднаний USB-каналом з міні-комп'ютером Raspberry Pi, що дає змогу виконувати обмін даними через Serial протокол. Замість Raspberry Pi може використовуватися звичайний домашній комп'ютер чи ноутбук, які підтримують опрацювання програмних кодів мови Python і забезпечують доступ до інтернету.

Плата Arduino запрограмована на контроль усіх компонентів розумного будинку та обмін необхідною інформацією з комп'ютером. Своєю чергою, комп'ютер безпосередньо взаємодіє з ботом Telegram. Він надсилає повідомлення користувачеві, які висвітлюються на його мобільному пристрої, а також отримує від користувача команди, які після опрацювання передаються платі Arduino. Програмне керування обміном повідомленнями і командами реалізоване засобами мови Python. Для організації комунікації з Telegram використовується бібліотека Aiogram. Обмін даними між комп'ютером і мікроконтролером плати Arduino здійснюється через Serial протокол із застосуванням бібліотеки Aioserial.

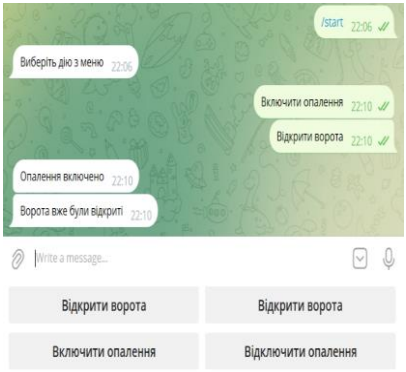
Основною складністю програмного рішення була необхідність забезпечити одночасне опрацьовування даних, що надходять як зі сторони Telegram, так і зі сторони Arduino. З цією метою створено два програмних обробники: перший – обробник Telegram бота – відповідає за організацію передачі даних, що надходять від Telegram месенджера до плати Arduino, а другий – обробник Arduino – керує даними, що передаються від Arduino до Telegram. Обидва обробники запускаються на одному ядрі процесора, що потребує узгодження їхньої взаємодії. Синхронна організація роботи обробників, коли запити опрацьовуються почергово, призводить до неефективного використання часу процесора, який буде простоювати в очікуванні відповіді від сервера Telegram.

Тому прийнято рішення застосувати асинхронну організацію взаємодії обробників, особливо ефективну при співпраці з сервером. У кожен момент часу процесор працює з одним із обробників. Якщо у цей час надходить запит до іншого обробника, то він заноситься у чергу. Як тільки дані першого обробника надсилаються на сервер, процесор перемикається на роботу з новим запитом.

Наведені нижче два скріншоти демонструють приклади "спілкування" користувача з системою розумного будинку. Рисунок 2а ілюструє випадок, коли користувач через месенджер Telegram надсилає певні інструкції системі розумного дому. Ці повідомлення надходять обробнику Telegram, який засобами бібліотеки Aioserial передає відповідну команду на плату Arduino, звідки запускаються потрібні виконавчі механізми. Мікроконтролер Arduino через свій обробник "звітує" Raspberry Pi про успішне чи невдале виконання

завдання, а користувач отримує відповідне повідомлення за допомогою бібліотеки Aiogram. Інший випадок – коли ініціатором спілкування є плата Arduino, наведено на рисунку 2б. Повідомлення від системи розумного будинку про сильний вітер доповнюється вбудованими кнопками вибору варіанту відповіді.

а



б

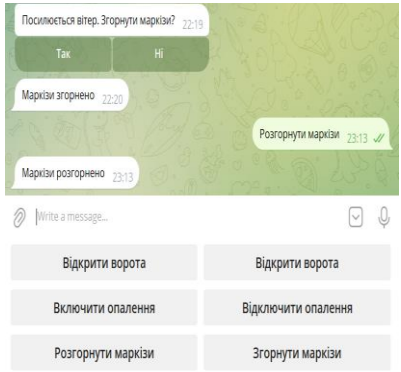


Рисунок 1 – Приклади обміну повідомленнями між користувачем і системою розумного будинку

Висновки. Можна зробити загальний висновок, що для організації обміну сповіщеннями між користувачем і системою розумного будинку необов'язково використовувати централізований сервер. Задачу віддаленого керування можна успішно реалізувати з використанням месенджерів, *наприклад* таких, як Telegram. Застосування чат-ботів робить систему інформування ефективною і зручною для користувачів. Водночас недоліком Telegram є те, що він може бути неконфіденційним і не гарантує безпеку даних. З цієї причини, якщо є потреба передавати певні приватні чи секретні дані, то доцільно використовувати інший месенджер.

Інформаційні джерела

1. Number of users of smart homes worldwide from 2019 to 2028. URL: https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-in-the-world

2. Most Popular Messaging Apps (2025). URL: https://explodingtopics.com/blog/messaging-apps-stats

Напрям 10

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 621.396.6

ВИЯВЛЕННЯ БПЛА ЗА ДОПОМОГОЮ SDR HACKRF ONE

Олександр БІЛИК
Олександр МАРТИНЧУК
Кафедра ІКІ ім. В. В. Поповського Харківського національного університету радіоелектроніки, м. Харків, Україна.

Abstract. *This paper explores the methodology for detecting unmanned aerial vehicles (UAVs) using Software Defined Radio (SDR) HackRF. Special attention is given to the analysis of UAV radio signals, the detection process, and classification. Practical recommendations for using HackRF in resource-constrained conditions are provided.*
Keywords: *SDR, HackRF, UAV, signal detection, radio frequency analysis.*

Анотація. *В роботі розглянуто підхід до виявлення безпілотних літальних апаратів (БПЛА) за допомогою програмно-визначеного радіо HackRF. Досліджено методику збору та аналізу радіосигналів БПЛА, визначено частотні діапазони їх роботи та надано рекомендації для практичного застосування.*
Ключові слова: *SDR, HackRF, БПЛА, виявлення сигналів, радіочастотний аналіз.*

У зв'язку зі стрімким розвитком технологій безпілотних літальних апаратів (БПЛА) зростає потреба у вдосконаленні засобів їх виявлення для забезпечення безпеки об'єктів критичної інфраструктури та військових об'єктів. Одним із ефективних інструментів для аналізу радіосигналів є програмно-визначене радіо (SDR). У роботі розглядається використання HackRF для виявлення та аналізу радіосигналів, що генеруються БПЛА.

Мета і завдання дослідження

Мета дослідження – розробка методики виявлення БПЛА за допомогою SDR HackRF. Для досягнення мети поставлено такі завдання:

– дослідити частотні діапазони, характерні для роботи БПЛА;

– розробити алгоритм збору, аналізу та класифікації сигналів;

– провести експериментальне дослідження ефективності виявлення БПЛА.

Методи дослідження

Для досягнення поставлених завдань використано методи спектрального аналізу, базовані на швидкому перетворенні Фур'є (FFT), а також алгори-

тми виявлення радіосигналів на основі патернів. У роботі застосовано програмне забезпечення GNU Radio та бібліотеки Python для обробки даних, отриманих від HackRF.

Результати дослідження

1. Частотні діапазони БПЛА

Більшість БПЛА використовують такі частотні діапазони:

– 2.4 ГГц (Wi-Fi) – для управління і передачі даних;

– 5.8 ГГц – для передачі відеосигналів.

2. Алгоритм виявлення сигналів

Розроблено алгоритм, який включає:

– сканування радіочастотного спектру;

– аналіз сигналів за допомогою FFT;

– виявлення сигналів, характерних для БПЛА, за допомогою бази даних патернів.

Нижче наведено приклад структури програми на Python із використанням бібліотеки GNU Radio:

```
import numpy as np
from gnuradio import analog, blocks, filter, gr, fft
from rtlsdr import RtlSdr
CENTER_FREQ = 2.4e9 # Центральна частота (2.4 ГГц)
SAMPLE_RATE = 2.048e6 # Швидкість дискретизації
BANDWIDTH = 20e6 # Ширина смуги
GAIN = 40 # Підсилення
class UAVDetector(gr.top_block):
def __init__(self):
gr.top_block.__init__(self)
# Налаштування SDR
self.sdr = blocks.rtlsdr_source()
self.sdr.set_center_freq(CENTER_FREQ)
self.sdr.set_sample_rate(SAMPLE_RATE)
self.sdr.set_bandwidth(BANDWIDTH)
self.sdr.set_gain(GAIN)
# Обробка сигналу
self.fft = fft.fft_vcc(1024, True, (window.hamming(1024)), True)
self.sink = blocks.vector_sink_c()
self.connect(self.sdr, self.fft, self.sink)
def detect_uav(self):
self.start()
samples = self.sink.data() # Отримуємо дані
spectrum = np.abs(np.fft.fft(samples))
```

```
self.stop()
self.wait()
# Виявлення сигналів на частотах БПЛА
if self.detect_signal(spectrum):
print("БПЛА виявлено!")
else:
print("Сигналів БПЛА не виявлено.")
def detect_signal(self, spectrum):
# Пошук характерних сигналів БПЛА
thresholds = [2.401e9, 5.8e9] # Частоти управління/відео
for freq in thresholds:
if any(abs(spectrum – freq) < 0.1e9):
return True
return False
if __name__ == "__main__":
detector = UAVDetector()
detector.detect_uav()
```

3. Експериментальні результати

Тестування системи на основі HackRF проведено в умовах експлуатації. Було успішно виявлено радіосигнали, що відповідали управлінню та передачі даних БПЛА. Система продемонструвала високу точність на відстані до 300 м, хоча чутливість знижувалася при наявності перешкод.

Висновки. HackRF є ефективним та доступним засобом для виявлення БПЛА в умовах обмежених ресурсів. Розроблена методика дозволяє ідентифікувати радіосигнали, характерні для БПЛА, з використанням аналізу частотних діапазонів і шаблонів сигналів. Подальші дослідження можуть бути зосереджені на впровадженні методів машинного навчання для підвищення точності класифікації.

Інформаційні джерела

1. Ali H. et al. UAV Signal Detection Using SDR Technology. IEEE Communications Magazine, 2023.

2. Smith J. SDR for Beginners: Exploring the Radio Spectrum. O'Reilly Media, 2022.

3. Білик О. С., Мартинчук О. О. Огляд методів виявлення БПЛА з використанням ортогонально-поляризованих шумоподібних радіосигналів та технології SDR. Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023) : матеріали дев'ятої Міжнародної науково-технічної конференції, 7 грудня 2023 р. – Харків : ХНУРЕ, 2023. – С. 52–56.

4. Білик О. С., Використання технології sdr в методах пасивної радіолокації та радіорозвідки // 27-й Міжнародний молодіжний форум "Радіоелектроніка та молодь у XXI столітті". Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2023. – С. 37–38.

УДК 004.7

АНАЛІЗ СУЧАСНИХ ПРОГРАМНО-АПАРАТНИХ РІШЕНЬ ДЛЯ IP-ТЕЛЕФОНІЇ

***Віктор ГНАТЮК*[1, 2]**
***Іван ГОРБАЧОВ*[1]**

[1]Національний авіаційний університет, м. Київ, Україна.
[2]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, м. Київ, Україна.

Abstract. *In this article, a study and systematization of relevant software and hardware solutions for IP telephony used in the modern business environment have been conducted. As a result of the research, key characteristics and functionalities of various IP telephony solutions have been identified, including software and hardware platforms, cloud solutions, and hybrid systems. An assessment of the advantages and disadvantages of each solution has been carried out.*

Keywords: *IP telephony, PBX, IP-PBX.*

Анотація. *У роботі проведено дослідження та систематизацію актуальних програмно-апаратних рішень для IP-телефонії, що використовуються в сучасному бізнес-середовищі. У результаті дослідження визначено ключові характеристики та функціональні можливості різних рішень для IP-телефонії, включаючи програмні та апаратні платформи, хмарні рішення та гібридні системи, здійснено оцінку переваг та недоліків кожного з рішень.*

Ключові слова*: IP-телефонія, PBX, IP-АТС.*

Актуальність використання IP-телефонії зростає у сучасному бізнес-середовищі завдяки її гнучкості, економічній ефективності та численним функціональним можливостям. Серед основних чинників, які визначають актуальність IP-телефонії можливо виділити наступні [1–10]: економічна ефективність; масштабованість та гнучкість, уніфіковані комунікації; мобільність та віддалений доступ; розширені функції; інтеграція з контакт-центрами; забезпечення якості обслуговування (QoS); захист та безпека; аналітика та контроль; підтримка нових технологій; тощо.

З огляду на це, метою роботи є дослідження та систематизація актуальних програмно-апаратних рішень для IP-телефонії, що використовуються в сучасному бізнес-середовищі. У результаті дослідження буде визначено ключові характеристики та функціональні можливості різних рішень для IP-телефонії, включаючи програмні та апаратні платформи, хмарні рішення та гібридні системи, здійснено оцінку переваг та недоліків кожного з рішень, враховуючи такі аспекти, як економічна ефективність, масштабованість, безпека, інтеграція з існуючими системами та користувацький досвід. Про-

ведено порівняння сучасних програмно-апаратних рішень за визначеними критеріями, що допоможе обрати оптимальне рішення для своїх потреб. Визначено тенденції розвитку IP-телефонії та її вплив на сучасні комунікаційні технології, а також проаналізовано перспективи інтеграції нових технологій, таких як штучний інтелект і автоматизація, у системи IP-телефонії. Також, буде надано рекомендації щодо вибору оптимальних рішень для різних типів підприємств в залежності від їх специфіки, що сприятиме підвищенню ефективності комунікацій і якості обслуговування клієнтів.

Сучасні програмно-апаратні рішення для IP-телефонії зазвичай включають кілька ключових компонентів (рис. 1): IP-телефони (апарати, які підтримують VoIP (Voice over IP) і дозволяють здійснювати дзвінки через Інтернет). VoIP шлюзи (пристрої або програми, що дозволяють інтегрувати традиційні телефонні мережі (PSTN) з IP-телефонією). Private Branch Exchange (програмне або апаратне забезпечення, яке керує внутрішніми дзвінками в організації і забезпечує маршрутизацію зовнішніх дзвінків). Системи управління дзвінками (програмне забезпечення для моніторингу, аналізу та управління дзвінками, включаючи функції запису, аналітики та управління чергами). Системи інтеграції з CRM (інтеграція IP-телефонії з системами управління відносинами з клієнтами для покращення обслуговування клієнтів). Системи управління безпекою (використання шифрування (*наприклад*, SRTP) та захист від атак (*наприклад*, SIP-трафік) для забезпечення безпеки дзвінків). Мережеве обладнання (роутери, комутатори та точки доступу, оптимізовані для обробки VoIP-трафіку). Клієнтське програмне забезпечення (програмні телефони, які дозволяють здійснювати дзвінки через комп'ютер або мобільний пристрій). Віртуальні телефонні системи (хмарні рішення, які надають всі функції телефонії без необхідності локального обладнання).

Ці компоненти взаємодіють між собою для забезпечення ефективної та якісної IP-телефонії.

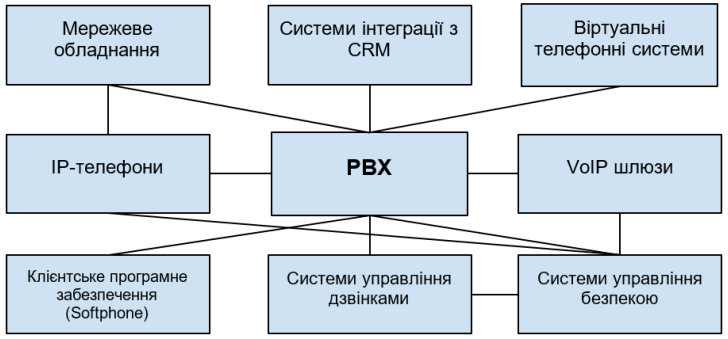


Рисунок 1 – Компоненти сучасних програмно-апаратних рішень для IP-телефонії

Сучасні програмно-апаратні рішення для IP-телефонії включають в себе різноманітне обладнання та програмні платформи, які забезпечують якісний зв'язок, ефективне управління, масштабованість і безпеку. Здійснимо порівняння сучасних програмно-апаратних рішень для IP-телефонії [11–18].

Таблиця 1.

Порівняння сучасних програмно-апаратних рішень для IP-телефонії

Рішення	*Тип*	*Масштабованість*	*Інтеграція з іншими сервісами*	*Безпека*	*Ціна*
Asterisk (IP PBX)	Програмне	Висока	Так	Шифрування, ACL	Безкоштовно / Ліцензія
3CX (IP PBX)	Програмне	Висока	Так	Шифрування, ACL	Ліцензія
Cisco CUCM (IP PBX)	Програмно-апаратне	Висока	Так	SBC, шифрування	Висока
Yealink IP-телефони	Апаратне	Середня	Обмежена	Шифрування	Середня
Cisco IP-телефони	Апаратне	Середня	Обмежена	Шифрування	Висока
Grandstream VoIP шлюзи	Апаратне	Середня	Обмежена	VPN, шифрування	Середня
Cisco VG шлюзи	Апаратне	Середня	Обмежена	VPN, шифрування	Висока
Microsoft Teams (UC)	Програмне	Висока	Так	Шифрування, ACL	Ліцензія
Zoom Phone (UC)	Програмне	Висока	Так	Шифрування, ACL	Ліцензія
RingCentral (Хмарна VoIP)	Хмарне	Висока	Так	SBC, шифрування	Абонентська плата
8x8 (Хмарна VoIP)	Хмарне	Висока	Так	SBC, шифрування	Абонентська плата
Polycom RealPresence Trio	Апаратне	Середня	Обмежена	Шифрування	Висока

Висновки. Таким чином, вибір оптимального рішення для IP-телефонії залежить від низки чинників, таких як специфіка бізнес-потреб, бюджет, кількість користувачів, вимоги до безпеки та інтеграції з іншими сервісами. Ось кілька ключових аспектів, які слід врахувати: тип бізнесу та масштаб (для невеликих підприємств, які потребують базових функцій, програмні рішення, такі як Asterisk або 3CX, можуть бути найкращим вибором завдяки

своїй економічності і високій масштабованості, для середніх та великих компаній з більш складними потребами в комунікації, таких як інтеграція з CRM-системами або високий рівень безпеки, оптимальними можуть бути Cisco CUCM або рішення на базі Microsoft Teams); інтеграція з існуючими системами (якщо компанія вже використовує певні програмні рішення, важливо обрати IP-телефонію, яка легко інтегрується з ними. *Наприклад*, Microsoft Teams та Zoom Phone забезпечують хорошу інтеграцію з офісними додатками, що може бути критично важливим для колективної роботи); безпека (якщо безпека є пріоритетом, рішення, такі як Cisco CUCM, які підтримують шифрування та додаткові заходи безпеки (SBC), можуть бути кращими. Також важливо врахувати можливості VPN та шифрування в інших рішеннях, таких як Grandstream VoIP шлюзи); цінова політика (вибір рішення також залежить від бюджету. Безкоштовні або недорогі варіанти, такі як Asterisk, можуть бути привабливими для стартапів або малих бізнесів. Водночас, якщо бізнес готовий інвестувати в довгострокові рішення з високою якістю обслуговування, варто розглянути платні рішення, такі як Cisco або RingCentral); мобільність та доступність (хмарні рішення, такі як RingCentral або 8x8, пропонують високу мобільність та доступність, що особливо важливо для компаній з віддаленими командами або філіями).

Інформаційні джерела

1. Василенко В. В., Литвин А. С. “Аналіз ефективності IP-телефонії у корпоративних мережах”. Науково-технічний журнал 15, №2 (2021). – С. 23–29.

2. Сидоренко М. І., Кузьменко Т. Г. “Забезпечення якості обслуговування в системах VoIP”. Телекомунікаційні та інформаційні технології 12, №4 (2022). – С. 67–74.

3. Johnson D. “Unified Communications and Collaboration in Modern Enterprises”. Journal of Telecommunication Systems & Management 31, №1 (2023). – С. 101–115.

4. Попов О. П., Дорошенко І. В. “Інтеграція уніфікованих комунікацій у системи IP-телефонії”. Інформаційні технології та засоби зв’язку 28, №3 (2022). – С. 48–55.

5. Cisco Systems. “Cisco Unified Communications Manager (CUCM): Deployment Guide”. Cisco White Paper, 2023.

6. Романов П. С. “Сучасні технології IP-телефонії для бізнесу”. Науковий вісник інформаційних та комунікаційних технологій 19, №2 (2021). – С. 35–43.

7. Microsoft Corporation. “The Benefits of Using Microsoft Teams for Unified Communications”. Microsoft Research, 2022.

8. Poly (Plantronics, Inc. & Polycom). “Polycom RealPresence Trio: Solution Overview”. Poly White Paper, 2023.

9. RingCentral. “Cost Efficiency and Scalability in Cloud-Based VoIP Solutions”. RingCentral Technical Report, 2023.

10. Микитенко А. В., Коваленко Н. Г. “Безпека голосових комунікацій у системах IP-телефонії”. Кібербезпека та захист інформації 9, №1 (2022). – С. 14–22.

11. Cisco Systems. “Cisco Unified Communications Manager (CUCM) Documentation”. Cisco White Paper, 2023.

12. Microsoft Corporation. “Microsoft Teams Unified Communications Features”. Microsoft Research, 2022.

13. Poly (Plantronics, Inc. & Polycom). “Polycom RealPresence Trio: Solution Overview”. Poly White Paper, 2023.
14. Grandstream Networks. “Grandstream VoIP Gateways Technical Manual”. Grandstream Documentation, 2023.
15. Yealink. “Yealink IP Phones: Features and Specifications”. Yealink Official Documentation, 2023.
16. RingCentral. “Cloud-Based VoIP Solutions: Features and Pricing”. RingCentral Technical Report, 2023.
17. TechRadar. “Best VoIP Solutions for 2023: A Comparative Review”. TechRadar, 2023.
18. G2. “User Reviews and Ratings of Modern IP Telephony Solutions”. G2, 2023.

УДК 004.738.5

МЕТОДИ ОПТИМІЗАЦІЇ РОБОТИ КОНТАКТ ЦЕНТРУ

***Віктор ГНАТЮК*[1, 2]**
***Олег БАТРАК*[1]**
***Михайло ГОЛОВАНЬ*[1]**
[1]Національний авіаційний університет, м. Київ, Україна.
[2]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, v/ Київ, Україна.

Abstract. *This paper investigates the main characteristics of mass service systems and analyzes methods for optimizing the operation of contact centers, including: intelligent query routing, the use of chatbots and automation, extending working hours and flexible scheduling, implementing an omnichannel strategy, load forecasting and resource planning, offloading part of the workload to other channels, improving the query prioritization system, and training personnel.*
Keywords: *automation; contact center; chatbot; mass service system; efficiency.*

Анотація. *У роботі досліджено основні характеристики систем масового обслуговування, проведено аналіз методів оптимізації роботи контакт-центру, серед яких: інтелектуальна маршрутизація запитів, використання чат-ботів та автоматизації, розширення робочого часу та гнучкий графік, реалізація омніканальної стратегії, прогнозування навантаження та планування ресурсів, перенесення частини навантаження на інші канали, удосконалення системи пріоритезації запитів та навчання персоналу.*
Ключові слова*: автоматизація; контакт-центр; чат-бот; система масового обслуговування; ефективність.*

Актуальність теми оптимізації діяльності контакт-центру зростає в умовах швидко змінюваного ринку послуг та зростаючих очікувань споживачів. Контакт-центри є ключовими елементами в управлінні взаємовідно-

синами з клієнтами (CRM), оскільки вони забезпечують перший рівень взаємодії та можуть суттєво впливати на рівень задоволеності клієнтів.

Сучасні дослідження підкреслюють важливість інтеграції новітніх технологій, таких як штучний інтелект (AI) і автоматизація, для покращення ефективності роботи контакт-центрів. *Наприклад*, дослідження показують, що впровадження AI може знизити час очікування на зв'язок та підвищити швидкість обробки запитів [1]. Також, згідно з роботою [2], оптимізація бізнес-процесів через аналіз даних і прогнозування попиту дозволяє зменшити витрати та покращити якість обслуговування.

Крім того, актуальність теми зумовлена змінами в поведінці споживачів: сьогодні клієнти очікують швидкого та зручного обслуговування через різноманітні канали комунікації. Відповідно, контакт-центри повинні адаптуватися до цих нових умов, щоб залишатися конкурентоспроможними [3].

Таким чином, дослідження оптимізації роботи контакт-центрів не лише актуальне, але й необхідне для забезпечення конкурентоспроможності підприємств у сучасному бізнес-середовищі.

З огляду на це, метою даної роботи є оптимізація роботи контакт центру задля підвищення ключових показників його діяльності.

Сучасні контакт центри являють собою системи масового обслуговування, зважаючи на це розглянемо модель системи масового обслуговування типового контакт центру.

Модель *M/M/N* – це модель масового обслуговування, яка використовується в теорії черг для моделювання систем, де клієнти надходять у випадкові моменти часу, обслуговуються і покидають систему [4–8]. У моделі *M/M/N* зазначається:

– *M* (Markovian): розподіл часу між прибуттями запитів (параметр λ) є експоненційним або, що рівнозначно, процесом Пуассона, тобто запити надходять випадковим чином з середньою швидкістю прибуття λ.

– *M* (Markovian): розподіл часу обслуговування (параметр μ) також є експоненційним, тобто час, необхідний для обслуговування запиту, є випадковим з середньою швидкістю μ.

– *N*: кількість каналів обслуговування (або операторів). Ця модель припускає, що в системі є N паралельних каналів обслуговування.

Модель M/M/N використовується для опису систем, де обслуговування здійснюється декількома операторами одночасно, а запити надходять випадково. Вона корисна для оцінки таких показників, як середній час очікування в черзі, коефіцієнт завантаження операторів, ймовірність того, що клієнт буде чекати, тощо.

Основні характеристики *M/M/N* моделі:

– розподіл прибуття клієнтів та часу обслуговування;

– *N* каналів обслуговування;

– інтенсивність надходження та обслуговування;

– час очікування в черзі.

Ця модель часто використовується для аналізу контакт-центрів, черг в банках, мережевих серверів і інших систем, де є багато паралельних каналів обслуговування, і метою є оцінка часу обслуговування або ймовірності очікування клієнтів.

Методи оптимізації роботи контакт-центру. Оптимізація роботи контакт-центру під час пікового навантаження може бути здійснена кількома методами [9–11]: інтелектуальна маршрутизація запитів, використання чат-ботів та автоматизації, розширення робочого часу та гнучкий графік, реалізація омніканальної стратегії, прогнозування навантаження та планування ресурсів, перенесення частини навантаження на інші канали, удосконалення системи пріоритезації запитів та навчання персоналу.

Висновки. Таким чином, у роботі досліджено основні характеристики систем масового обслуговування, проведено аналіз методів оптимізації роботи контакт-центру, серед яких: інтелектуальна маршрутизація запитів, використання чат-ботів та автоматизації, розширення робочого часу та гнучкий графік, реалізація омніканальної стратегії, прогнозування навантаження та планування ресурсів, перенесення частини навантаження на інші канали, удосконалення системи пріоритезації запитів та навчання персоналу. Ці підходи можуть допомогти знизити навантаження та забезпечити стабільну роботу контакт-центру навіть під час піків активності.

Інформаційні джерела

1. Jain R., Gupta A., & Singh P. (2021). The impact of artificial intelligence on customer service efficiency in contact centers. Journal of Service Research, 24(3), pp. 321–336. URL: https://doi.org/10.1177/1094670520931234.

2. Smith J., Brown T., & Lee K. (2022). Optimizing business processes in contact centers through data analytics. International Journal of Operations Management, 45(2), pp. 178–195. URL: https://doi.org/10.1108/IJOM-11-2021-0645

3. Kumar V., & Reinartz W. (2016). Creating enduring customer value. Journal of Marketing, 80(6), pp. 36–68. URL: https://doi.org/10.1509/jm.15.0427.

4. Gross D., Shortle J. F., Thompson J. M., & Harris C. M. (2018). Fundamentals of Queueing Theory (5th ed.). Wiley.

5. Whitt W. (2021). Understanding the M/M/N Queue: Insights and Approximations. Queueing Systems, 98(3), pp. 321–345. doi:10.1007/s11134-021-09651-2.

6. Kim S., & Choi J. (2022). Performance Analysis of M/M/N/K Queueing Models with Customer Retrial. Stochastic Models, 38(1), pp. 45–63. doi:10.1080/15326349.2022.1968456.

7. Medhi J. (2017). Stochastic Models in Queueing Theory (2nd ed.). Academic Press.

8. Abate J., & Whitt W. (2020). Transient Behavior of the M/M/N Queue. Operations Research Letters, 48(3), pp. 234–240. doi:10.1016/j.orl.2020.02.003.

9. Mehrotra V., & Profozich D. (2022). Optimization Techniques for Call Centers: Balancing Customer Satisfaction and Operational Efficiency. Operations Research Perspectives, 9, 100214. doi:10.1016/j.orp.2022.100214.

10. Gans N., & Zhou Y.-P. (2021). Dynamic Routing and Scheduling in Multi-Channel Contact Centers. European Journal of Operational Research, 295(1), pp. 238–251. doi:10.1016/j.ejor.2021.03.017.

11. Khodakarami V., & Chan Y. E. (2023). AI-Driven Chatbot Integration for Customer Service Optimization in Contact Centers. Journal of Service Management, 34(2), pp. 123–140. doi:10.1108/JOSM-11-2022-0387.

УДК: 004.7:004.415.2:004.056.5

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ І МОДЕЛЕЙ ОЦІНКИ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Роман ГАМРЕЦЬКИЙ
Віктор ГНАТЮК
Державний університет "Київський авіаційний інститут", м. Київ, Україна.

Abstract*. The study analyzes software quality assessment models, including ISO/IEC 25010, Six Sigma, FURPS, and others, in the context of modern technologies (IoT, 5G, AI). Improvements are proposed through integrating new metrics, automation, and hybrid approaches to ensure effective adaptation to technological challenges.*

Keywords*: software quality, quality assessment models, ISO/IEC 25010, CMMI, Six Sigma, FURPS, TQM, GQM, metrics, automation, IoT, 5G, artificial intelligence.*

Анотація. *Дослідження аналізує моделі оцінки якості програмного забезпечення, зокрема ISO/IEC 25010, Six Sigma, FURPS та інші, в умовах сучасних технологій (IoT, 5G, AI). Запропоновано вдосконалення через інтеграцію нових метрик, автоматизацію та гібридні підходи, що забезпечить ефективну адаптацію до технологічних викликів.*

Ключові слова: *якість програмного забезпечення, моделі оцінки якості, ISO/IEC 25010, CMMI, Six Sigma, FURPS, TQM, GQM, метрики, автоматизація, IoT, 5G, штучний інтелект.*

Інформаційно-комунікаційні системи (ІКС) є основою сучасних цифрових технологій, забезпечуючи ефективну взаємодію між організаціями, технологіями та кінцевими користувачами. Якість програмного забезпечення (ПЗ), що лежить в основі цих систем, критично впливає на їхню продуктивність, безпеку, надійність та зручність використання. З розвитком технологій, таких як хмарні обчислення, IoT, 5G і штучний інтелект, зростають вимоги до оцінки якості ПЗ. Це зумовлює необхідність оновлення підходів та інструментів оцінювання, що дозволить ефективніше адаптувати ПЗ до нових умов і викликів.

Метою цього дослідження є порівняння сучасних моделей оцінки якості ПЗ для визначення їх переваг, недоліків і сфер застосування, а також пропонування напрямків вдосконалення методів оцінки. Такі моделі як, ISO/IEC 25010, Capability Maturity Model Integration (CMMI), McCall, Boehm, Six Sigma, FURPS/FURPS+, Dromey, Total Quality Management (TQM), Goal-Question-Metric (GQM), ISO/IEC 9126 та ін., є важливими інструментами для аналізу якості, але їх адаптація до нових умов залишається актуальним завданням.

У сучасному контексті виникає потреба не тільки в оцінці базових характеристик ПЗ, таких як функціональна придатність чи продуктивність, а й у врахуванні параметрів кібербезпеки, енергоефективності, масштабованості, зручності використання та ін.

ISO/IEC 25010 визначає якість через характеристики: функціональна придатність, продуктивність, зручність використання, надійність, безпека та переносність [1]. Вона є універсальною і широко застосовується для оцінки складних систем, однак потребує значних ресурсів для впровадження.

CMMI зосереджується на зрілості процесів розробки, забезпечуючи структурований підхід до управління якістю [2]. Хоча вона ефективна для покращення процесів, впровадження може бути складним для малих організацій через вимоги до ресурсів.

Модель McCall класифікує характеристики на операційні, ревізійні та перехідні, що допомагає оцінювати базові аспекти якості [3]. Проте вона не враховує сучасних технологічних викликів, таких як кібербезпека та масштабованість.

Модель Boehm має ієрархічну структуру, орієнтовану на супроводжуваність, переносимість і зручність використання [4]. Її недоліком є відсутність інтеграції із сучасними методами автоматизації та недостатня увага до нових технологічних тенденцій.

Six Sigma фокусується на статистичному аналізі для мінімізації дефектів і підвищення продуктивності [5]. Це робить її ефективною для великих організацій, але менш адаптивною для оцінки зручності використання та інших якісних аспектів.

FURPS/FURPS+ враховує функціональність, зручність, продуктивність, надійність і супроводжуваність, додаючи аспекти масштабованості та розширюваності [6]. Вона детально описує вимоги до системи, але може бути складною у застосуванні через велику кількість параметрів.

Модель Dromey концентрується на зв’язку між властивостями ПЗ та атрибутами якості, допомагаючи розробникам зрозуміти, як конкретні рішення у коді впливають на загальну якість продукту [7].

Total Quality Management (TQM) є філософією управління, спрямованою на постійне покращення якості у всіх аспектах організації через залучення всіх співробітників. У контексті ПЗ, TQM інтегрує принципи якості на всіх етапах життєвого циклу розробки, але потребує значних змін у корпоративній культурі та процесах [8].

Goal-Question-Metric (GQM) – підхід, який передбачає визначення цілей, формулювання запитань для оцінки досягнення цих цілей та встановлення метрик для вимірювання відповідей. GQM дозволяє налаштовувати процес оцінки якості відповідно до специфічних потреб проекту, але вимагає глибокого розуміння процесів і ресурсів для збору даних [9].

ISO/IEC 9126, попередник ISO/IEC 25010, складається з шести основних характеристик: функціональність, надійність, зручність використання, ефективність, супроводжуваність та переносність [10]. Хоча він був широко використовуваний, з розвитком технологій виникла потреба в його оновленні.

Оцінка якості ПЗ базується на формальних метриках, які дозволяють забезпечити об'єктивність і точність аналізу. У моделі ISO/IEC 25010 загальна якість ПЗ (Q) визначається як середньозважене значення оцінок характеристик:

$$Q = \frac{w_1 C_1 + w_2 C_2 + ... + w_n C_n}{\sum_{i=1}^{n} w_i}, \qquad (1)$$

де C_i – оцінка і-ї характеристики (*наприклад*, функціональної придатності, продуктивності тощо); w_i – вага і-ї характеристики, яка визначається залежно від пріоритетів системи.

Характеристики розраховуються в залежності від контексту та вимог до проведення оцінювання, *наприклад* характеристика функціональної повноти (ступінь, до якої всі необхідні функції реалізовані), може бути оцінена за формулою:

$$P_{completness} = \frac{Number\ of\ implemented\ functions}{Total\ number\ of\ required\ functions} \times 100\% \qquad (2)$$

Наприклад, якщо реалізовано 18 із 20 необхідних функцій, то

$$P_{completness} = \frac{18}{20} \times 100\% = 90\% \qquad (3)$$

Окрім цього, Six Sigma фокусується на статистичному аналізі для мінімізації дефектів і підвищення продуктивності, що робить її ефективною для великих організацій, але менш адаптивною для оцінки зручності використання.

Методологія Six Sigma спрямована на мінімізацію дефектів, використовуючи метрику *DPMO* (Defects Per Million Opportunities):

$$DPMO = \frac{Number\ of\ defects}{Total\ opportunities\ for\ defects} \times 1000000\% \qquad (4)$$

Наприклад, якщо у 10000 одиниць продукції знайдено 50 дефектів із 20 можливостями для дефектів на одиницю:

$$DPMO = \frac{50}{10000 \times 20} \times 1000000 = 250 \qquad (5)$$

Проведений аналіз демонструє, що ISO/IEC 25010 є стандартизованою і універсальною, тоді як Six Sigma ефективна для мінімізації дефектів у складних системах. CMMI забезпечує структурований підхід до управління якістю, але її впровадження складне для малих організацій. FURPS/FURPS+ виділяється фокусом на користувацькому досвіді, а McCall корисна для базового аналізу якості. TQM сприяє покращенню якості на рівні організації, але потребує значних змін у корпоративній культурі. GQM дозволяє адаптувати метрики під конкретні цілі, але потребує чіткого визначення цих цілей та ресурсів для їх досягнення.

Сучасні виклики, такі як інтеграція IoT, хмарних технологій, мікросервісної архітектури, а також зростання вимог до кібербезпеки, потребують адаптації існуючих моделей:

– IoT – моделі мають враховувати низьку затримку передачі даних і масштабованість систем;

– Кібербезпека – інтеграція метрик конфіденційності (6) та цілісності (7) дозволяє забезпечити захист даних.

$$P_{confidentiality} = \frac{Number\ of\ \ unauthorized\ \ attempts\ blocked}{Total\ \ unauthorized\ \ access\ attempts} \times 100\% \qquad (6)$$

$$P_{\text{int}egrity} = \frac{Number\ of\ \ unaltered\ \ recors}{Total\ \ records} \times 100\% \qquad (7)$$

Практичне впровадження цих моделей і підходів демонструє їхню ефективність. ISO/IEC 25010 широко використовується у корпоративних системах, Six Sigma ефективна для оптимізації процесів у виробничих системах, а FURPS/FURPS+ забезпечує якісний аналіз користувацького досвіду в мобільних додатках. Однак жодна з моделей не є універсальною, що підкреслює важливість розробки гібридних підходів, які об’єднують сильні сторони існуючих моделей.

Варіантами вдосконалення можуть бути:

– гібридна модель – інтеграція сильних сторін моделей ISO/IEC 25010 та Six Sigma для забезпечення всебічного аналізу;

– автоматизація – використання штучного інтелекту для автоматичного збору метрик і прогнозування якості;

– нові метрики – розробка індикаторів енергоефективності та екологічної стійкості, зокрема для IoT.

Висновки. Порівняльний аналіз показує, що вдосконалення методів оцінки якості ПЗ є необхідним кроком для забезпечення відповідності сучасним викликам. Інтеграція нових технологій, адаптація підходів до потреб користувачів та використання автоматизації дозволять зробити оцінку якості більш ефективною, точною та релевантною в умовах розвитку ІКС.

Інформаційні джерела

1. ISO/IEC 25010:2023. Systems and software engineering–Systems and software Quality Requirements and Evaluation (SQuaRE)–System and software quality models, International Organization for Standardization, Geneva, Switzerland, 2023.
2. CMMI Institute. CMMI® for Development, Version 2.0. CMMI Institute, 2018.
3. McCall J. A., Richards P. K., and Walters G. F. Factors in Software Quality, General Electric, 1977.
4. Boehm B. W. et al., Characteristics of Software Quality, North-Holland, 1978.
5. Pyzdek T. and Keller P. A. The Six Sigma Handbook, 4th ed., McGraw-Hill, 2014.
6. RGrady. B. Practical Software Metrics for Project Management and Process Improvement, Prentice Hall, 1992.
7. Dromey R. G. A model for software product quality. IEEE Transactions on Software Engineering, vol. 21, no. 2, pp. 146–162, 1995.
8. Oakland J. S. Total Quality Management: Text with Cases, Butterworth-Heinemann, 1995.
9. Basili V. R. and Rombach H. D. The TAME project: Towards improvement-oriented software environments. IEEE Transactions on Software Engineering, vol. 14, no. 6, pp. 758–773, 1988.
10. ISO/IEC 9126-1:2001. Software engineering–Product quality–Part 1: Quality model, International Organization for Standardization, Geneva, Switzerland, 2001.

УДК 004.9:614.8

РОЗРОБЛЕННЯ СЕРВІСУ ПОШУКУ НАЙБЛИЖЧИХ МЕДЗАКЛАДІВ НА ОСНОВІ ГЕОЛОКАЦІЇ

Тарас ПАНЬКІВ
Юрій БОРЗОВ

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The paper examines the development of a service for finding the nearest medical facilities based on the user's geolocation data. The system architecture, data processing algorithms, and key functionalities are presented. The proposed approach improves the accessibility of medical services by providing a user-friendly interface and accurate results.*

Keywords: *geolocation, medical facilities, search service, data processing.*

Анотація. *У роботі розглянуто процес розроблення сервісу пошуку найближчих медичних закладів на основі геолокаційних даних користувача. Представлено архітектуру системи, алгоритми обробки даних та основні функціональні можливості сервісу. Запропонований підхід покращує доступність медичних послуг, забезпечуючи зручний інтерфейс та точність результатів.*

Ключові слова: *геолокація, медичні заклади, пошуковий сервіс, обробка даних.*

Сучасні інформаційні технології стрімко інтегруються в різні сфери життя, зокрема й у процес надання різноманітних послуг. Одним із важливих напрямків є створення сервісів, які допомагають оперативно знаходити медичні заклади поблизу, що особливо актуально у великих містах. Основною метою розробки такого сервісу є забезпечення користувачів можливістю швидко отримувати інформацію про найближчі медичні установи з урахуванням їхнього поточного місцезнаходження та необхідних послуг. Для досягнення цієї мети важливо дотримуватися кількох ключових вимог: точна обробка геолокаційних даних, зручний та інтуїтивно зрозумілий інтерфейс, інтеграція з іншими додатками та базами даних.

Сервіс будується на архітектурі, що включає кілька основних компонентів. Насамперед це модуль збору геоданих, який використовує GPS або інші технології для визначення координат користувача. Інформація про медичні установи зберігається в базі даних, яка містить їхнє місцезнаходження, спеціалізацію, графік роботи та контактні дані. Пошукові алгоритми, зокрема методи на основі k-найближчих сусідів (k-NN), забезпечують швидкий і точний підбір відповідних закладів. Взаємодія з користувачами відбувається через месенджери, що дозволяє легко та зручно отримувати необхідну інформацію.

Процес пошуку закладів включає кілька послідовних етапів (рис. 1). Спочатку визначаються координати користувача, після чого формується запит до бази даних із заданими критеріями, такими як спеціалізація чи максимальна відстань. Далі обчислюються відстані до всіх закладів у зоні досяжності, результати сортуються, і користувач отримує найбільш релевантні варіанти. Для підвищення продуктивності роботи сервісу застосовуються технології кешування запитів та оптимізації обчислень, що скорочує час відповіді.

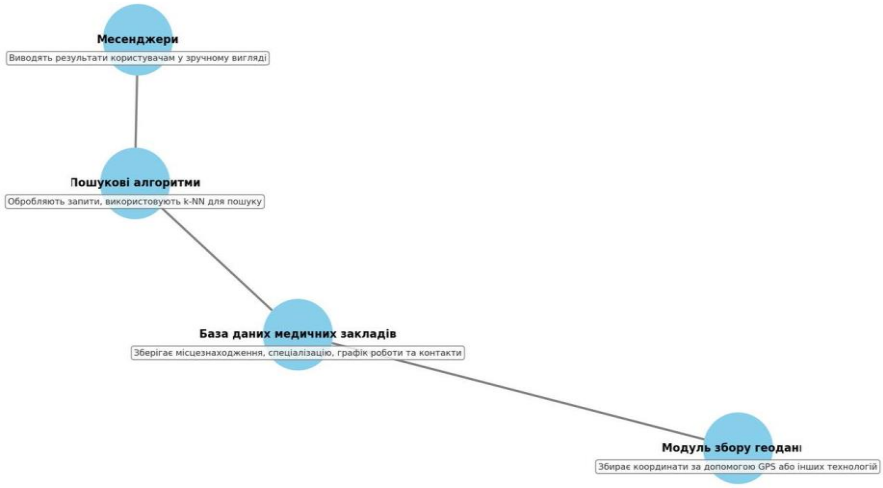


Рисунок 1 – Архітектура сервісу

Сервіс було реалізовано на основі стеку технологій:
– Back-end: Python (Django), Microsoft Exel;
– Front-end: ReactJS;
– геолокаційний сервіс: Google Maps API.

Тестування проводилося на основі геоданих Львівської області. Результати показали високу точність пошуку (95%) та швидкість обробки запитів (у середньому 0,8 с) (рис. 2).

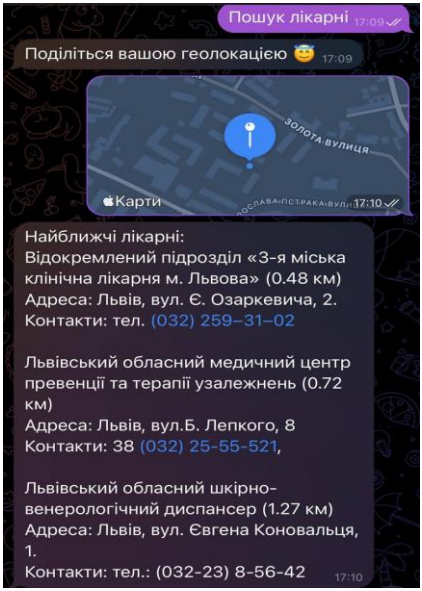


Рисунок 2 – Результати проведеного тестування

Висновки. Розроблений сервіс дозволяє користувачам швидко знаходити найближчі медичні заклади, використовуючи геолокаційні дані. Це спрощує доступ до медичних послуг та підвищує їх оперативність. Перспективний розвиток системи може включати впровадження функцій персоналізації, таких як врахування особливих потреб користувачів, та інтеграцію з іншими інформаційними сервісами для забезпечення більш широкого спектра можливостей.

Інформаційні джерела

1. Крамаренко О. М., Лисенко Т. П. Геолокаційні сервіси у сучасних інформаційних системах. – Київ: Науковий вісник, 2021.
2. Smith J., Brown T. Geolocation and its application in healthcare. – New York: TechPress, 2020.
3. Google Maps API Documentation. URL: https://developers.google.com/ maps/ documentation.

УДК 338.488.2:640.43:004(045)

АВТОМАТИЗАЦІЯ В РЕСТОРАННОМУ БІЗНЕСІ: СУЧАСНІ РІШЕННЯ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ТА СЕРВІСУ

Оксана ГРОМИК
Луцький національний технічний університет, м. Луцьк, Україна.

Abstract. *The publication considers the use of information and computer technologies for managing restaurant establishments in order to increase the efficiency of their activities. The focus is on the automation of business processes, which contributes to the optimization of costs, ensuring reliable financial accounting, effective cost control and improving data exchange between departments. The roles and tasks of personnel that should be supported by automated systems are determined. A review of existing programs for automating the front office and back office is conducted, and it is also proposed to switch to free software, implement electronic document management and expand the capabilities of online communication to increase management efficiency. It is noted that Poster POS can become the basis for creating a full-fledged automated management system that will optimize all business processes, reduce costs and improve the quality of guest service.*

Keywords: *restaurant establishments, restaurant business, hospitality industry, information and computer technologies, efficiency.*

Анотація. *У публікації розглянуто використання інформаційних та комп'ютерних технологій для управління закладами ресторанного господарства з метою підвищення ефективності їхньої діяльності. Акцентовано увагу на автоматизації бізнес-процесів, що сприяє оптимізації витрат, забезпеченню надійного обліку фінансів, ефективному контролю витрат і поліпшенню обміну даними між підрозділами. Визначено ролі та задачі персоналу, які мають підтримуватись автоматизованими системами. Проведено огляд існуючих програм для автоматизації фронт-офісу та бек-офісу, а також програмне забезпечення, впровадження яких забезпечить електронний документообіг і розширить можливості онлайн-комунікації для підвищення ефективності управління. Зазначено, що Poster POS може стати основою для створення повноцінної автоматизованої системи управління, яка дозволить оптимізувати всі бізнес-процеси, знизити витрати та підвищити якість обслуговування гостей.*

Ключові слова: *заклади ресторанного господарства, ресторанний бізнес, індустрія гостинності, інформаційні та комп'ютерні технології, ефективність.*

Сучасні технології стрімко змінюють ресторанний бізнес. Автоматизація процесів обслуговування не лише знижує витрати, а й підвищує ефективність роботи закладів ресторанного господарства. Завдяки автоматизації замовлення виконуються швидше, помилки мінімізуються, а гості отримують кращий сервіс. Хоча початкові інвестиції можуть бути значними, з часом вони окупаються завдяки зростанню прибутковості. Сьогодні багато

ресторанів все ще використовують ручні методи обліку, що гальмує їхній розвиток. Тому переваги автоматизація у закладах ресторанного господарства – це шлях до успіху в сучасному ресторанному бізнесі.

Дослідження впровадження інформаційних комп'ютерних технологій у роботі закладів ресторанного господарства відображенні у низці вітчизняних та закордонних науковців. Зокрема: Мельниченко С. В., Миронов Ю. Б., Олійник О. В., Рябенька М. О., Шестакова А. В., Пашута М. Т., Даниленко О. В., Зоценко Л. М., Братіцел М. Л., Роглєв Х. Й., Бухаліса Л. Д. [1–6]. Проте питання застосування інформаційних технологій у закладах ресторанного господарства залишається предметом наукового дослідження.

Мета дослідження є аналіз процесу впровадження автоматизованих систем управління в закладах ресторанного господарства.

При проведенні дослідження використовувались загальнонаукові методи: порівняння, узагальнення, аналізу, синтезу та систематизації.

Інформаційні технології відіграють вирішальну роль у формуванні стратегії розвитку закладів ресторанного господарства а також забезпечують високу швидкість пошуку необхідної інформації. Сучасні технології стали невід'ємною частиною успішного бізнесу в сфері гостинності. Завдяки їм заклади ресторанного господарства можуть оперативно реагувати на зміни ринку та забезпечувати високий рівень обслуговування гостей.

Власники закладів ресторанного господарства звертають досить велику увагу на якість обслуговування та сервіс, доволі суворіше ставляться до відбору персоналу, а також застосовують новітні технології та інновації, щоб виділятись на ринку конкурентів швидкістю обслуговування, якістю страв, "фішкою" закладу та його стилем.

З ростом чисельності ресторанів стрімко посилюється і конкуренція, що неминуче призводить до необхідності ефективно і раціонально використовувати наявні ресурси. У цих умовах для успішного ведення бізнесу необхідно інвестувати в засоби та інструменти його підтримки і розвитку. Один з основних інструментів розвитку ресторанного бізнесу - це сучасна система автоматизації ресторанів.

У зв'язку з активним розвитком ресторанного господарства, з підвищенням конкуренції, інтерес до автоматизації управління постійно зростає.

Автоматизація кафе і ресторану дозволяє оптимізувати документообіг, забезпечити порядок на складі. Всі дані зберігаються в єдиній системі. В даний час, особливо у великих містах, автоматизація ресторану є абсолютно необхідним рішенням для того, щоб зробити свій заклад кращим.

Сучасна система автоматизації ресторану - це професійна система управління рестораном, багатофункціональна і легко модернізована. Метою автоматизації є підвищення ефективності управління рестораном, прискорення обслуговування і мінімізація можливих зловживань, особливо крадіжок. Значна частка успіху складається з відмінного сервісу і оперативної

роботи персоналу. Саме можливості автоматизації ресторану дозволяють оптимально поєднувати швидкість і якість.

Переваги автоматизованого ресторану перед іншими подібними закладами:

– висока якість сервісу і швидкість обслуговування гостей;

– відсутність помилок при оформленні замовлення;

– обробка і передача замовлення у автоматичному режимі;

– абсолютний контроль всіх процесів від моменту прийому замовлення до його виконання;

– можливість безперервно відстежувати фінансові результати роботи закладу.

Poster POS - це комплексна система автоматизації для закладів ресторанного господарства, яка включає в себе функції CRM, онлайн-каси, управління складом та фінансами. Варто окреслити основні переваги та недоліки використання цієї системи (табл. 1).

Таблиця 1.

Переваги та недоліки впровадження автоматизованої системи Poster POS у діяльність закладу ресторанного господарства

Переваги		*Недоліки*	
Основні переваги провадження	*Значення*	*Основні недоліки провадження*	*Значення*
Універсальність і адаптивність	Poster POS підходить для бізнесу будь-якого розміру, від маленьких кав'ярень до великих мереж ресторанів. Система дозволяє легко адаптувати функціонал під потреби конкретного закладу	Залежність від інтернет-з'єднання	Хоча система може працювати в офлайн-режимі, для повноцінної роботи потрібне стабільне інтернет-з'єднання. Це може стати проблемою в закладах з поганим сигналом
Безконтактні технології	Впровадження QR-меню дозволяє гостям робити замовлення та оплачувати їх без контакту з офіціантом, що підвищує швидкість обслуговування і комфорт для гостей	Технічні проблеми	Деякі користувачі відзначають періодичні технічні збої, такі як помилки при створенні звітів, що може ускладнити процес управління
Автоматизація процесів	Система забезпечує контроль за запасами, ведення фінансової звітності, аналіз продажів та управління програмами лояльності. Це дозволяє власникам бізнесу зосередитися на розвитку закладу	Вартість підписки	Після безкоштовного тестового періоду необхідно обрати тарифний план, що може бути дорогим для малих бізнесів

Зручний інтерфейс	Poster має інтуїтивно зрозумілий інтерфейс, що спрощує навчання персоналу і роботу з системою. Також доступні мобільні додатки для різних ролей у ресторані (офіціанти, менеджери тощо)		
Технічна підтримка	Користувачі отримують постійну підтримку і можливість безкоштовного оновлення програмного забезпечення		

Poster POS є потужним інструментом для автоматизації ресторанного бізнесу з численними перевагами, такими як універсальність, безконтактні технології та зручний інтерфейс. Однак, потенційні користувачі повинні враховувати можливі недоліки, пов'язані з залежністю від інтернету та технічними проблемами.

Висновки. Отже, для досягнення максимальної ефективності ресторанного бізнесу необхідно відмовитися від часткової автоматизації окремих функцій і перейти до комплексного впровадження сучасних технологій. Системи типу Poster POS можуть стати основою для створення повноцінної автоматизованої системи управління, яка дозволить оптимізувати всі бізнес-процеси, знизити витрати та підвищити якість обслуговування гостей.

Інформаційні джерела

1. Громик О. М. Особливості розвитку індустрії гостинності в Україні // Ресторанний і готельний консалтинг. Інновації : наук. зб. / Київ. нац. ун-т культури і мистецтв. Київ: Вид. цент КНУКІМ. 2023. Т. 6, № 2. – С. 184–198. URL: http://restaurant-hotel.knukim.edu.ua/article/view/291701.

2. Громик О. М. Оцінювання стану розвитку готельного бізнесу в Україні // Ресторанний і готельний консалтинг. Інновації : наук. зб. / Київ. нац. ун-т культури і мистецтв. Київ: Вид. цент КНУКІМ. 2022. Т. 5, № 1. – С. 52–62. URL: http://restaurant-hotel.knukim.edu.ua/issue/view/15613

3. Мельниченко С., Михайліченко Г., Мезенцева Г. Туристична сфера: вихід з карантину. Зовнішня торгівля: економіка, фінанси, право. 2020. № 6. – С. 23–34. Серія: Економічні науки.

4. Миронова М. І., Миронов Ю. Б. Показники ефективності діяльності підприємств індустрії гостинності. Матеріали Всеукраїнської науковопрактичної конференції (м. Черкаси, 16–17 квітня 2020 р.). Черкаси, 2020. – С. 517–520.

5. Олійник О. В., Шестакова А. В., & Ярмолюк Д. І. (2023). Напрями цифровізації ресторанного бізнесу. Економіка, управління та адміністрування. – С. 15–21. URL: https://doi.org/10.26642/ema-2023-1(103).

6. Рябенька М. Впровадження інформаційних комп'ютерних технологій у рестоарнний бізнес. Економіка та суспільство. 2022. (41). URL: https://doi.org/10.32782/2524-0072/2022-41-65

УДК 004.73.

ВДОСКОНАЛЕННЯ УПРАВЛІННЯ КОМП'ЮТЕРНОЮ МЕРЕЖЕЮ ІНТЕРНЕТ ПРОВАЙДЕРА

Володимир ОСТРОВЕРХИЙ
В'ячеслав МОЛОШНИЙ
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article is dedicated to the improvement of computer network management for internet service providers in the context of modern cyber threats. It examines issues related to network topology selection, including physical and logical aspects, as well as methods for ensuring data security, particularly through the use of cryptographic protection tools. Special attention is given to the trade-off between security levels and network performance, a key challenge for administrators. The role of active and passive network equipment in the efficient functioning of networks is also discussed, especially regarding scalability and reliability. Recommendations for improving network management contribute to enhancing data security and transmission efficiency.*

Keywords: *computer network management, internet provider, network topology, data security, cryptography, information protection, active and passive network equipment, network efficiency, scalability, performance, cyber threats.*

Анотація. *Доповідь присвячена вдосконаленню управління комп'ютерними мережами інтернет-провайдерів у контексті сучасних кіберзагроз. Зокрема, розглядаються питання вибору топології мережі, включаючи фізичні та логічні аспекти, а також методи забезпечення безпеки даних, зокрема через використання криптографічних засобів захисту. Окрема увага приділяється вибору між рівнем захисту і продуктивністю мережі, що є важливою задачею для адміністраторів. Обговорюється також роль активного та пасивного мережевого обладнання в ефективному функціонуванні мережі, зокрема в умовах масштабованості та надійності. Рекомендації щодо вдосконалення управління мережами сприяють підвищенню безпеки та ефективності передачі даних.*

Ключові слова: *управління комп'ютерною мережею, інтернет-провайдер, топологія мережі, безпека даних, криптографія, захист інформації, активне і пасивне мережеве обладнання, ефективність мережі, масштабованість, продуктивність, кіберзагрози.*

Актуальність дослідження. Розвиток технологій призводить до появи нових технологій, методів та засобів несанкціонованого доступу та кібератак, що вимагає прийняття нових рішень по удосконаленню роботи комп'ютерних мереж. Тому дослідження процесів управління комп'ютерною мережею інтернет провайдера з метою удосконалення її роботи є актуальною задачею сьогодення.

Виклад основного матеріалу. Однією з основних завдань при побудові нової комп'ютерної мережі є вибір топології мережі. На вибір топології

впливає багато факторів, включаючи: методи управління мережею, необхідне мережеве обладнання та його характеристики, кінцева мета побудованої мережі та її масштабованість, відстань, з якої може передаватися інформація, тощо. Топологія локальної мережі підрозділяється на фізичні та логічні мережеві побудови [1].

Топологія фізичних з'єднань описує геометричне розташування локальних компонентів мережі, відображає структуру з'єднання між її основними елементами. Друга частина топології локальної мережі це її логічна структура, на рівнях логічної структури та логічного каналу.

Характер передачі інформації, характер з'єднань між робочими станціями і функціями даних про поширенні інформаційних сигналів між пристроями, визначається поширенням інформаційних сигналів між пристроями. Логічні канали керують передачею інформації між робочими станціями, у той же час логічна організація не завжди збігається з фізичною топологією мережі.

У сучасних комп'ютерах і комп'ютерних системах поняття безпеки є досить широким, це включає як забезпечення надійності комп'ютера, так і зберігання цінних даних [2].

Крім захисту мережі, адміністратори завжди стикаються з проблемою вибору між необхідним рівнем захисту і ефективною роботою мережі. Широко поширене, використання комп'ютерних технологій в автоматизованих системах обробки та управління інформацією. Це призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерній системі, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має ряд особливостей, пов'язаних з тим, що інформація не залежить від носія, може бути легко і швидко скопійована і передана по каналах зв'язку.

Вирішення проблеми. Для вирішення проблеми у мережі інформаційної безпеки можуть використовуватися два типи засобів, і програмне забезпечення.

Основним рішенням проблеми захисту інформації, яка передається по каналах зв'язку, є захист зашифрованих даних, що реалізується програмними, апаратними і апаратно-програмними засобами. На додаток до використання кожного методу окремо, можливо використовувати комбінацію апаратних і програмних механізмів захисту шифруванням. Найбільш поширеним методом є використання програмної реалізації криптографічних алгоритмів з апаратним сховищем ключів, що забезпечує високий рівень захисту за низькою ціною.

Зазвичай існує два типа мережевого обладнання, а саме активне і пасивне. Активне мережеве обладнання – це сукупність обладнання та інтелектуальних технічних засобів для передачі даних та обміну інформацією пристрій локальної мережі. До таких пристроїв належать маршрутизатори, керовані комутатори та апаратний мережевий екран. Пасивні мережеві пристрої включають пристрої, на які не поширюється інтелектуальна власність [3]. Це кабелі, розетки, концентратори, тощо.

Висновки. В умовах зростаючих кіберзагроз та розвитку технологій, удосконалення управління комп'ютерними мережами є ключовим аспектом

забезпечення надійності та функціональності інтернет-провайдерів. Правильний вибір топології мережі є базовою умовою її ефективності. Поєднання фізичних і логічних структур дозволяє досягти оптимального розподілу ресурсів і передачі даних. Надійний захист даних у мережі залежить від використання сучасних криптографічних методів, апаратних та програмних рішень. Комбінація цих підходів дозволяє забезпечити високий рівень безпеки при мінімальних витратах. Вибір між високим рівнем захисту і продуктивністю мережі є одним із ключових викликів для адміністраторів, що вимагає інтегрованих рішень. Ефективність роботи мережі значною мірою залежить від поєднання активного (маршрутизатори, комутатори) і пасивного (кабелі, роз'єми) обладнання, які відповідають вимогам масштабованості та надійності мережі. Поєднання ефективного управління, безпечної передачі даних і можливостей масштабування є основними складовими успішного функціонування сучасних комп'ютерних мереж. Ці фактори підкреслюють важливість постійного вдосконалення технологій і підходів до управління мережами для забезпечення їх надійності, безпеки та продуктивності.

Інформаційні джерела

1. Вдосконалення мережі інтернет провайдера. URL: https://naurok.com.ua/.(дата звернення 17.11.2024).

2. Управління мережею інтернет провайдера. URL: https://uk.wikipedia.org/wiki/. (дата звернення: 17.11.2024).

3. Конференції Державного університету "Житомирська політехніка". URL: https://conf.ztu.edu.ua/wp-content/uploads/2019/12/27-2.pdf (дата звернення: 17.11.2024).

УДК 621.396

ФУНКЦІОНУВАННЯ ЗАСОБІВ (СИСТЕМ) ЗВ'ЯЗКУ В ОРГАНАХ ТА ПІДРОЗДІЛАХ ДСНС УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Володимир ПИЛИПЕНКО
Юрій БОРЗОВ

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *Sustainable functioning and implementation of modern communication systems and means in the bodies and subdivisions of the SES of Ukraine is one of the strategic directions of the service and the State as a whole. The author analyzes the directions of development of information and communication technologies that facilitate the introduction of digital communication systems and the use of modern solutions to provide reliable communication channels for the bodies and subdivisions of the SES of Ukraine.*

Keywords: *State Emergency Service of Ukraine (SESU), communication channels, radio communication, digital communications, information system.*

Анотація. *Стале функціонування та запровадження сучасних систем та засобів зв'язку в органах та підрозділах ДСНС України є одним із стратегічних напрямків роботи служби і держави в цілому. Проаналізовано напрямки розвитку інформаційно-комунікаційних технологій, які сприяють впровадженню цифрових систем зв'язку і використання сучасних рішень для забезпечення надійними каналами зв'язку органи та підрозділи ДСНС України.*

Ключові слова: *ДСНС України, канали зв'язку, радіозв'язок, цифрові комунікації, інформаційна система.*

З початком повномасштабного вторгнення російських окупаційних військ на територію України перед Державною службою України з надзвичайних ситуацій (далі – ДСНС України) постало багато нових викликів, у тому числі ліквідації наслідків влучань російських ракет по житлових забудовах, кварталах. Це у свою чергу потребує не тільки використання пожежної та спеціальної рятувальної техніки, але й сучасних, надійних систем забезпечення сталого зв'язку як на місці ліквідації надзвичайних ситуацій, так і до прийому і обробки викликів на спецлінії 101 та Системи 112.

В умовах тотальних блекаутів і введення погодинних графіків відключень електропостачання, перед ДСНС України виникла гостра потреба в забезпеченні безперебійного та стабільного функціонування ІТ-інфраструктури, що включає надійне оброблення та зберігання даних, оперативне реагування на надзвичайні ситуації, а також захист критичних інформаційних систем від потенційних загроз і технічних збоїв. Фахівцями центрів оперативного зв'язку запроваджено ряд організаційних та технічних заходів щодо сталого й безперебійного зв'язку на всіх рівнях, починаючи від державного пожежно-рятувального поста до апарату ДСНС України, а саме:

– забезпечення усіх критичних вузлів відомчої мережі гарантованим резервним живлення (серверні кімнати, ЦОДи, ретранслятори радіозв'язку);

– налаштування та використання кількох каналів зв'язку (підключення декількох незалежних один від одного інтернет-провайдерів);

– використання супутникових комплектів Інтернет-доступу типу "Starlink";

– налаштування та використання каналів зв'язку від Державної служби спеціального зв'язку та захисту інформації України;

– впровадження резервних схем маршрутизації викликів на спецлінії 101, використовуючи ресурси операторів стільникового зв'язку, АТ "Укртелеком" та надавачів послуг із SIP-транкінгу.

Одним із ключових засобів зв'язку в умовах воєнного стану є забезпечення ДСНС України сучасним радіозв'язком, яке полягає у побудові відомчої цифрової радіомережі. Активне впровадження цифрового радіозв'язку дозволило повністю перебудувати логіку радіомереж ДСНС України, а також удосконалити взаємодію із іншими службами на всіх рівнях. Цифровий радіозв'язок забезпечив високу захищеність радіопередачі сигналу, відстежування та моніторинг місцезнаходження за допомогою GPS. *На прикладі*

впровадження цифрового радіозв'язку у місті Львові та Львівській області охоплення зони покриття становить близько 90%, з яких покриття стаціонарних радіостанцій – 99%, автомобільних і переносних – близько 80%. Менше охоплення, зазвичай, є у гірській місцевості, де за особливістю рельєфу, не завжди є можливість проходження радіохвиль. Надійність та охоплення великої зони покриття здійснено за рахунок встановлення базових станцій (радіоретрансляційного обладнання) та ретрансляторів. Кожний ретранслятор створює навколо себе "СОТУ" покриття, а "СОТИ" об'єднуються, створюючи територію покриття (рис 1).

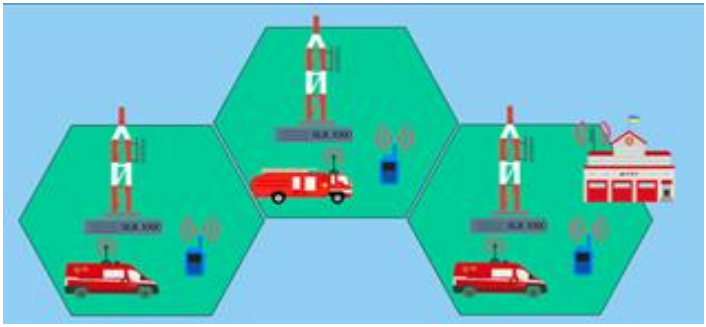


Рисунок 1 – Схематичний вигляд "Сот"

Системою цифрового радіозв'язку можна керувати за допомого серверу та спеціалізованого програмного забезпечення, яке називається "SMART PTT" (рис 2). Загалом PTT означає "Push-To-Talk", комунікаційну технологію, яка дозволяє користувачам натискати кнопку, щоб передавати свій голос через двосторонню радіостанцію або інший пристрій зв'язку. Smart PTT відноситься до версії цієї технології, яка містить додаткові функції та можливості, такі як відстеження місцезнаходження GPS, обмін миттєвими повідомленнями, групові виклики та інтеграція з іншими системами зв'язку.

ДСНС України активно впроваджує багаторівневу систему безперервного прийому та обробки викликів на лінії 101 із використанням новітніх методів побудови систем, які базуються на цифрових процесах доставки голосових дзвінків до кінцевого абонента. Використання цифрових IP АТС та SIP-транків провайдерів зв'язку в органах та підрозділах ДСНС України дозволяє гнучко налаштовувати під конкретні потреби того чи іншого підрозділу. Ця система включає в себе розділення серверної та мережевої інфраструктури географічно, а також забезпечення одночасно кількох незалежних каналів зв'язку, що мінімізує виведення з ладу спецлінії 101. У випадках локального пошкодження чи відсутності зв'язку із основними системами здійснюється автоматичне переключення на аналогові лінії центрального вузла АТ "Укртелеком". На сьогодні відмовитись повністю від використан-

ня мереж загального користування не можливо, так як це залишається зв'язком "останньої надії".

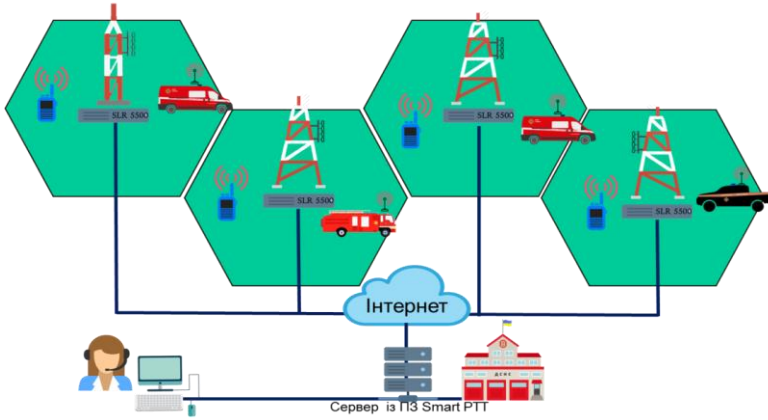


Рисунок 2 – Схематичний вигляд "SMART PTT"

Упровадження нових схем прийому і обробки екстрених викликів на лінії 101 дозволило забезпечити безперебійну роботу в умовах війни та тотальних відключень електроенергії, а використання волоконно-оптичних ліній зв'язку є сучасним і надійним рішенням.

Також, активно здійснюється впровадження сучасних інформаційно-аналітичних систем таких як: МІА: Облік і звіт, МІА: Здоров'я, Система автоматизованого документообігу АСКОД, Інтерактивний інспектор, Логістична інформаційна система. Всі ці системи створюють єдину екосистему в автоматизації робочих процесів, планування, обліку, контролю та аналізу ділових процесів управлінської, виробничої, фінансової та господарської діяльності.

Висновки. Таким чином, на основі викладеного матеріалу, можна стверджувати, що ефективне впровадження та використання сучасних засобів (систем) зв'язку в умовах війни в органах та підрозділах ДСНС України, забезпечує кращу взаємодію під час ліквідації наслідків ракетних влучань та надзвичайних ситуацій, а також гарантує сталий, безперебійний зв'язок та дозволяє ефективно використовувати сили та засоби за призначенням.

Інформаційні джерела

1. Дії підрозділів ДСНС України в умовах воєнного стану : навч. посіб. / ред. М. С. Коваль. Львів : ЛДУБЖД, 2023. 306 с.

2. Сайко В. Г., Амірханов Е. Д. Основи мереж цифрового радіозв'язку і радіодоступу нового покоління. К.: ДУТ, 2015. 77 с.

3. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX : станом на 8 листоп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

4. Gonçalves F. E. Configuration guide for Asterisk PBX. 2nd ed. 2007. 370 p.

Напрям 11

3D МОДЕЛЮВАННЯ ТА 3D ДРУК

УДК 004.925

3D МОДЕЛЮВАННЯ ТА 3D ДРУК – МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ

Назар ДУХНИЧ
Олександр ХЛЕВНОЙ
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The paper examines modern methods of 3D modeling, key 3D printing technologies, and the prospects for their application in various fields, such as industry, medicine, and culture.*
Key words*: 3D modeling, 3D printing, innovations, production, prototyping.*

Анотація. *В роботі розглянуто сучасні методи 3D моделювання, ключові технології 3D друку, а також перспективи їхнього застосування в різних галузях.*
Ключові слова*: 3D моделювання, 3D друк, інновації, виробництво, прототипування.*

Сьогодні 3D моделювання та 3D друк є важливими технологіями, які активно впливають на розвиток багатьох галузей. Їх використання дозволяє суттєво прискорити процеси створення нових продуктів, забезпечити економію ресурсів та підвищити якість кінцевих виробів.

3D моделювання є базовим етапом створення цифрових моделей, які використовуються для прототипування, симуляцій та створення готових виробів. У сфері промисловості тривимірні моделі дозволяють проектувати складні механічні деталі, зменшуючи кількість помилок на етапі виробництва. В архітектурі та дизайні 3D моделі дозволяють створювати візуалізації будівель, інтер'єрів або меблів, що значно полегшує узгодження проектів із замовниками.

Існує кілька основних технологій 3D друку:

– моделювання методом наплавлення (Fused Deposition Modeling, FDM);
– лазерна стереолітографія (Laser Stereolithography, SLA);
– селективне лазерне спікання (Selective Laser Sintering, SLS);

– селективне лазерне плавлення (Selective Laser Melting, SLM);

– пряме лазерне спікання металу (Direct Metal Laser Sintering, DMLS);

– вибіркове теплове спікання (Selective Heat Sintering, SHS);

– виготовлення об'єктів за допомогою ламінування (Laminated Object Manufacturing, LOM);

– метод багатоструминного моделювання (Multi Jet Modeling, MJM);

– електронно-променеве плавлення (Electron-beam Melting, EBM);

– кольоровий струминний друк (Color Jet Printing, CJP);

– цифрова світлодіодна проекція (Digital Light Processing, DLP).

Ці технології дозволяють друкувати об'єкти різної складності, забезпечуючи гнучкість у виборі матеріалів і швидкість виробництва.

Застосування 3D-друку в виробництві:

1. *Прототипування*. Швидке прототипування є не тільки другою назвою методики, але і початковою метою її розробки. Створення дослідних зразків за допомогою 3D друку значно скорочує час і витрати виробництва. Прототипування дозволяє наочно оцінити можливі недоліки виробу ще на етапі проектування і внести істотні зміни в конструкцію деталі ще до її остаточного затвердження.

2. Дрібносерійне виробництво. Властивості багатьох матеріалів дозволяють виробляти готові компоненти з мінімальними витратами. Порівняно з традиційними методами виробництва, дрібносерійне виробництво за допомогою 3D друку дуже вигідно з фінансової точки зору. Інтеграція 3D друку в автоматизовані виробничі системи дозволяє створювати складні вироби безпосередньо за допомогою цифрових моделей. Це значно спрощує процеси, такі як прототипування, та відкриває нові можливості для малосерійного виробництва.

3. Ремонт і відновлення. Проводити таку процедуру можна як самостійно, при наявності відповідних навичок і устаткування, так і в спеціалізованих сервісах 3D друку. Ремонт і відновлення пошкоджених деталей відбувається швидко, а наявність цифрової моделі компонента дозволяє заново віддрукувати його в будь-який час.

4. Виробництво функціональних моделей і готових компонентів. Одна з різновидів промислового застосування 3D друку – виробництво функціональних моделей і готових компонентів. Виготовлення виробів на 3D принтері з прозорого матеріалу дозволяє побачити роботу функціональної деталі "зсередини", що дуже корисно при розробці різних інженерних зразків. Крім того, широкий спектр різноманітних матеріалів для 3D друку перетворює її в повноцінний виробничий інструмент.

5. Побутові предмети. Будь-які побутові предмети можна надрукувати на 3D принтері. Перевага такого застосування в тому, що при розробці 3D моделей немає ніяких обмежень. Тобто, при бажанні проявити фантазію і створити щось оригінальне – всі карти в ваших руках. Завдяки новітній технології свій будинок можна прикрасити і зробити більш функціональним легко і недорого.

6. Іграшки та сувеніри. Сьогодні існує декілька цікавих проектів колективних 3D – друкованих ігор. Принтер з підтримкою друку декількома матеріалами дозволить виготовити ексклюзивні сувеніри.

7. Дизайнерські вироби. Художники, скульптори, модельєри і дизайнери зі всього світу використовують 3D друк для створення ексклюзивних предметів мистецтва, виготовити які стандартними методами було б неможливо. Такі дизайнерські вироби вражають своєю красою і оригінальністю, часто поєднуючи цифрове і традиційне мистецтво. Крім того, активно розробляються методики 3D друку одягу і взуття. Деякі моделі вже навіть надійшли в продаж, але про масове виробництво поки рано говорити.

Однією з найперспективніших сфер для 3D друку є медицина. Сьогодні технологія використовується для створення індивідуальних імплантатів, моделей органів для планування хірургічних операцій, а також для виготовлення протезів, максимально адаптованих до фізіологічних особливостей пацієнтів. У майбутньому можливе використання 3D друку для створення штучних органів із біосумісних матеріалів.

Застосування 3D друку дає змогу суттєво знизити виробничі витрати завдяки мінімізації кількості відходів і можливості локального виробництва. Крім того, використання матеріалів, що підлягають переробці, сприяє зменшенню негативного впливу на довкілля.

Висновки. 3D моделювання та 3D друк є одними з ключових технологій нашого часу. Їх застосування сприяє підвищенню продуктивності, зниженню витрат і вдосконаленню процесів у багатьох галузях. Застосування технологій 3D-друку в легкій промисловості – це величезний стрибок вперед, здатний вирішити низку проблем у легкій промисловості та підняти її на якісно новий рівень. Подальший розвиток цих технологій обіцяє ще більше можливостей для інновацій та покращення якості життя.

Інформаційні джерела

1. Технічна творчість. Сучасні технології в механіці / укл.: Скиба М. Є., Поліщук О. С., Онофрійчук В. І. – Хмельницький : ХНУ, 2016. – 214 с.

2. Сучасні види тривимірного друку. URL: https://3ddevice.com.ua/3d-%D0%B4%D1%80%D1%83%D0%BA/%D0%B2%D0%B8%D0%B4%D0%B8-3d-%D0%B4%D1%80%D1%83%D0%BA%D1%83/?

3. Перспективи технологій 3D друку. URL: https://mik.dcz.gov.ua/publikaciya/perspektyvy-tehnologiy-3d-druku

УДК 004.9

ВИКОРИСТАННЯ UNITY ДЛЯ 3D-МОДЕЛЮВАННЯ З ЕЛЕМЕНТАМИ ЛІНІЙНОГО ШИФРУВАННЯ

Максим ІВАНОВСЬКИЙ
Мирослава КУСІЙ
Кафедра прикладної математики і механіки Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *Considered the combination of Unity for creating 3D models and linear encryption. The main principles of such integration are described, and an example is provided. Practical aspects of applying this approach in various fields (gaming industry, engineering, medicine, education) are outlined. It is demonstrated that the integration of Unity with linear encryption ensures a basic level of security without significant impact on system performance. Conclusions are made regarding the advantages, disadvantages, and potential development paths of this method to enhance the security of 3D projects.*

Key words: *Unity, 3D models, linear encryption, information protection, encryption.*

Анотація. *Розглянуто поєднання Unity для створення 3D-моделей та лінійного шифрування. Описано основні принципи такої інтеграції та наведено приклад. Зазначено практичні аспекти застосування такого підходу в різних галузях (ігрова індустрія, інженерія, медицина,освіта). Показано, що з'єднання Unity з лінійним шифруванням забезпечує базовий рівень безпеки без істотного впливу на продуктивність системи. Зроблено висновки про переваги, недоліки та можливості шляхів розвитку цього методу для підвищення захищеності 3D-проектів.*

Ключові слова: *Unity, 3D-моделі, лінійного шифрування, захист інформації, шифрування.*

У сучасних реаліях надзвичайно актуальним є 3D-моделювання, яке активно використовується в різних сферах: від створення ігор до різноманітних візуалізацій та інженерних симуляцій. Із розвитком цифрових інструментів для 3D-моделювання постала серйозна проблема: як захистити конфіденційну інформацію, вбудовану в тривимірні проекти? *Наприклад*, у медичних або інженерних додатках витік даних можна призвести до серйозних наслідків. Одним із перспективних інструментів для 3D-моделювання є Unity – потужний ігровий рушій і універсальна платформа для створення 3D додатків. Але, якщо поєднати його можливості з методами шифрування? Такий підхід дозволить нам, не лише моделювати віртуальні світи, а й забезпечувати їхній захист від несанкціонованого доступу. Спробуємо розглянути, як ці дві технології можуть працювати разом для досягнення нових висот у сфері безпеки й моделювання.

Unity широко застосовується для розробки 2D- та 3D-додатків. Завдяки своїй універсальності та підтримці програмування на C++, Unity є ідеа-

льним інструментом для створення інтерактивних середовищ та тривимірних моделей [1].

Основними можливостями Unity є:

– розробка реалістичних 3D-сцен з підтримкою фізики;

– інтеграція сторонніх даних;

– підтримка скриптів для складних взаємодій;

– кросплатформенність (Android, iOS, ПК та інші) [2].

Лінійний шифр – це метод шифрування, у якому використовується лінійна математична операція (лінійне перетворення чи матричне обчислення) [3]. Його переваги:

– простота реалізації;

– висока швидкість роботи;

– мінімальне навантаження на систему.

Хоча лінійне шифрування не є настільки безпечним, як складні алгоритми (AES чи RSA), воно чудово підходить для завдань, де важливий швидкий доступ до даних і базовий рівень захисту.

Спробуємо поєднати Unity для 3D-моделювання з лінійним шифруванням. Для цього нам знадобиться декілька етапів:

1. *Розробка 3D-моделі*.

На першому етапі створюється 3D-модель у середовищі Unity. Це може бути архітектурна структура, об'єкт віртуальної реальності або сцена з інтерактивними елементами. Ми, для прикладу, створимо 3D-модель деяких приміщень Львівського державного університету безпеки життєдіяльності (рис. 1).

Рисунок 1 – Об'єкти створені за допомогою технології 3D-моделювання у середовищі Unity

2. *Інтеграція даних у модель*.

Дані, пов'язані з моделлю (*наприклад*, координати, конфігурації чи текстові підказки), зберігаються у вигляді масивів або файлів у проекті Unity.

3. *Шифрування даних*

Дані перед інтеграцією шифруються за допомогою лінійних операцій [4]. *Наприклад* (рис. 2).

Рисунок 2 – Шифрування даних за допомогою лінійних операцій

4. *Розшифрування в реальному часі*.

Під час запуску додатка Unity дешифрує дані, коли це потрібно. *Наприклад*, інформація про вхід може розшифруватися лише після користувача або при активації певного елемента сцени.

5. *Контроль доступу*.

Шифрування дозволяє створити рівні доступу до частин моделі чи функціональної добавки. *Наприклад*, неавторизовані користувачі бачать лише загальні елементи, тоді як додаткові дані стануть доступними після введення ключа.

Наведемо приклади, де можна використовувати Unity з елементами шифрування:

– віртуальна реальність: у медичних візуалізаціях можна захистити персональні дані пацієнта, які використані в моделях органів чи процедур;

– інженерні симуляції: шифрування дозволяють приховати конфіденційні технічні характеристики в моделях обладнання або об'єктів інфраструктури;

– ігрова індустрія: у відеоіграх лінійне шифрування можна використовувати для захисту даних персонажів, карт чи сценаріїв від стороннього доступу;

– навчальні симуляції: у навчальних додатках дані можуть бути захищені, щоб гарантувати коректність і точність інформації, яку підтримують користувачі.

Звичайно, у даному підході є свої переваги та недоліки.

До переваг ми відносимо:

– простота реалізації;

– висока швидкість обробки;

– гнучкість у налаштуваннях для різних потреб.

Недоліки:

– обмежений рівень безпеки (для більш складних і критичних проєктів можна комбінувати лінійне шифрування з такими алгоритмами, як AES, RSA.

– потреба в додаткових механізмах для захисту від підбору ключа.

Висновки. Інтеграція 3D-моделювання в Unity та лінійного шифрування відкриває нові можливості для їх використання в різних галузях, таких як ігрова індустрія, медицина, інженерія та освіта. Такий підхід дозволяє створити не лише інтерактивні, а й захищені додатки, які особливо важливі в сучасному світі, де безпека даних відіграє ключову роль. Окрім цього, такий підхід дозволяє урізноманітнити та зробити більш цікавим навчальний процес для здобувачів освіти відповідних спеціальностей.

Інформаційні джерела

1. Unity Technologies. Посібник користувача Unity. URL: https:// docs.unity3d.com/Manual/index.html, останнє оновлення: 2024.

2. Сміт К. Розробка 3D-ігор за допомогою Unity. – Packt Publishing, 2019.

3. Стасюк Марта Математичні основи криптографії (Спеціальні розділи математики) : навчальний посібник. Львів : ЛДУ БЖД, 2021. – 216 с.

4. Львівський державний університет безпеки життєдіяльності: віртуальний університет. URL: https://virt.ldubgd.edu.ua/pluginfile.php/132457/mod_resource/content/5/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%20%D0%90%D0%A8.pdf

УДК 004.925

АКТУАЛЬНІСТЬ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ 3D-ВІЗУАЛІЗАЦІЇ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ МАЙБУТНІХ ФАХІВЦІВ

Віра ДОВБНЯК

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The growing role of digital technologies in the educational process is contributing to the integration of innovative teaching methods. 3D visualisation is a powerful tool that can significantly improve the understanding of complex concepts and processes in various fields of knowledge.*

Key words*: 3D technology, visualisation, training, innovation.*

Анотація. *Зростання ролі цифрових технологій в освітньому процесі сприяє інтеграції інноваційних методів навчання. 3D-візуалізація є потужним інструментом, що дозволяє значно покращити розуміння складних концептів та процесів у різних галузях знань.*

Ключові слова: *3D технології, візуалізація, навчання, інновації.*

Сучасні технології змінюють підходи до професійної підготовки. Технологія 3D-візуалізації відкриває нові можливості для моделювання, аналізу та відтворення об’єктів у віртуальному середовищі, підвищуючи ефективність навчання та сприяючи глибшому розумінню складних концепцій. Актуальність дослідження зумовлена потребою у впровадженні сучасних технологій, які відповідають вимогам ринку праці та сприяють формуванню висококваліфікованих фахівців.

Переваги використання 3D-візуалізації у навчанні включають кілька ключових аспектів. По-перше, це інтерактивність та наочність, які забезпечуються через створення реалістичних моделей, що дозволяють студентам взаємодіяти з об’єктами та краще засвоювати навчальний матеріал. По-друге, використання 3D-візуалізації сприяє поглибленому розумінню завдяки можливості спостерігати об’єкти з різних перспектив, що розвиває просторове мислення. І, нарешті, така технологія знижує складність сприйняття, роблячи складні технічні процеси та теоретичні концепції більш зрозумілими через їх візуальне представлення.

Сфери застосування 3D-візуалізації у підготовці фахівців охоплюють широкий спектр галузей. У сфері інженерних наук та архітектури ця технологія використовується для моделювання конструкцій, механізмів і інфраструктурних об’єктів, що сприяє ефективному проектуванню та їх вивчен-

ню. У медицині 3D-візуалізація дозволяє створювати моделі органів і анатомії людини, забезпечуючи якісну підготовку майбутніх лікарів і хірургів. У мистецтві та дизайні вона допомагає створювати віртуальні моделі для проектування та аналізу естетичних рішень. Крім того, у фізиці та хімії 3D-технології застосовуються для візуалізації молекул, атомів і фізичних явищ, що сприяє більш глибокому розумінню та проведенню експериментів.

Розвиток критичних навичок у майбутніх рятувальників значно посилюється завдяки використанню 3D-візуалізації. Ця технологія сприяє формуванню аналітичних здібностей, розвитку креативності та вдосконаленню технічних навичок студентів. Завдяки можливості моделювати й аналізувати складні системи, студенти отримують практичний досвід, що готує їх до ефективного реагування на реальні професійні виклики.

Для створення та інтеграції 3D-візуалізації у навчальний процес використовуються популярні програмні засоби, такі як Autodesk, Blender та Unity3D, а також сучасні платформи для розробки 3D-контенту. Крім того, значний потенціал мають технології віртуальної (VR) та доповненої реальності (AR), які дозволяють створювати інтерактивні навчальні середовища, що максимально наближають студентів до реальних умов роботи.

Попри значні переваги, впровадження 3D-візуалізації супроводжується певними викликами. Серед них – високі вимоги до комп'ютерної техніки та програмного забезпечення для забезпечення якісної візуалізації. Також існує потреба у підготовці викладачів, які володіють навичками роботи з новітніми технологіями. Додатковою перешкодою є висока вартість впровадження та обмежена доступність цих технологій у багатьох навчальних закладах, що вимагає пошуку ефективних шляхів фінансування та оптимізації витрат.

Висновки. Застосування 3D-візуалізації в професійній підготовці майбутніх фахівців має значний потенціал для підвищення ефективності навчального процесу. Важливо продовжувати інтеграцію таких технологій у освітній простір для забезпечення високого рівня підготовки фахівців, готових до викликів сучасного світу.

Інформаційні джерела

1. Angelov Angel, Smieja Tomasz & Styczynski Z. A. (2007). Acceptance of 3D Visualizations Methods for Learning and Training in the Area of Electrical Engineering.

2. Batı Ayşe. (2022). 3D modelling for realistic training and learning. Turkish Journal of Biochemistry. doi: 10.1515/tjb-2019-0182.

Напрям 12

МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СИСТЕМ

UDC 519.6

APPLICATION OF THE STOCHASTIC SIR MODEL TO CYBERSECURITY THREATS MODELING

Serhiy SEMENYUK
Lviv Polytechnic National University, Lviv, Ukraine.

Abstract. *Malware propagation is a significant cybersecurity threat, with malicious software such as viruses, worms, and ransomware capable of spreading across networks. In this work, we consider deterministic and stochastic versions of the SIR model to describe the threat propagation. The stochastic models incorporate random fluctuations in user behavior, providing a more realistic understanding of malware dynamics.*
Keywords: *malware propagation, stochastic process, mathematical model, SIR model, Code Red worm.*

Анотація. *Розповсюдження зловмисного програмного забезпечення є значною загрозою кібербезпеці, оскільки шкідливе програмне забезпечення, як-от віруси, хробаки та програми-вимагачі, здатне поширюватися мережами. У цій роботі ми розглядаємо детерміновану та стохастичну версії моделі SIR для опису поширення загрози. Стохастичні моделі включають випадкові коливання в поведінці користувачів, забезпечуючи більш реалістичне розуміння динаміки зловмисного програмного забезпечення.*
Ключові слова: *розповсюдження шкідливих програм, стохастичний процес, математична модель, модель SIR, хробак Code Red.*

Malicious software can spread rapidly across networks, causing substantial damage. Therefore, modeling malware propagation is critical for understanding its dynamics, including how it spreads between systems, the speed of infection, and which systems are most at risk.

Traditionally, deterministic models, such as epidemic models, have been used to analyze malware propagation. The biological approach to modeling malware began with [1] and gained attention following the outbreak of Code Red in 2001 (see [2] for details). While these models provide useful insights for basic prediction, they fail to capture the complexities of real-world networks, including random factors like varying communication patterns, differences in system defenses, and unpredictable user actions. To address these limitations, stochastic models, which incorporate randomness, offer a more realistic perspective on malware dynamics.

Stochastic evolution models are mathematical frameworks that account for random processes affecting system behavior [3]. Originally applied in biology [4], economics, and physics, these models have proven increasingly relevant for studying malware propagation.

This work explores deterministic and stochastic SIR models, using data from the Code Red outbreak to compare their effectiveness and lay the groundwork for understanding stochastic processes.

The Code Red worm, first detected on July 15, 2001, targeted computers running Microsoft's IIS web server. By July 19, an enhanced variant, Code Red v2, emerged, infecting over 350,000 systems within nine hours. The worm propagated by scanning the Internet for vulnerable systems, exploiting an IIS vulnerability, and self-installing on those systems. Its rapid spread led to severe disruptions, including a major Denial of Service (DoS) attack.

The dataset analyzed in this study was sourced from packet headers collected from CAIDA's /8 network telescope [5], TCP SYN packet timestamp/IP address pairs received by two /16 networks at Lawrence Berkeley Laboratory, and sampled netflows from a router monitoring upstream traffic at CAIDA's /8 network telescope.

This dataset, spanning July 18, 2001 (19:00 UTC) to July 20, 2001 (2:10 UTC), was aggregated into 10-second intervals, yielding 11,218 observations of infected systems.

In the simplest form, the SIR model can be described the following system [6]:

$$\begin{cases} \frac{dS}{dt} = -\beta IS, \\ \frac{dI}{dt} = \beta IS - \gamma I, \\ \frac{dR}{dt} = \gamma I. \end{cases}$$

where: N – total number of hosts considered (we have N =359104 from the model data); S – number of susceptible/vulnerable hosts; I – number of infected hosts. Each infected host can infect a susceptible with probability bt during time t; R – the number of recovered hosts.

The Least Square Estimation method is applied to determine the optimal value of the parameters b, g. This method aims to fit the model to observed data by minimizing the sum of the squared differences between the observed values and the model's predicted values.

Assuming $I(0) = 1$ (i.e., there was only a single host infected at the beginning) and $R(0) = 0$ (i.e., there were no recovered hosts at the beginning), the best-fit value would be $b = 0.0021368324$, $g = 2.585 \times 10^{-6}$ (see Figure 1 for the result).

Having these estimations, a basic reproduction ratio can be calculated. R_0= b / g ≈ 826,6. This ratio is derived as the expected number of new infections (these new infections are sometimes called secondary infections) from a single infection to which all hosts are susceptible.

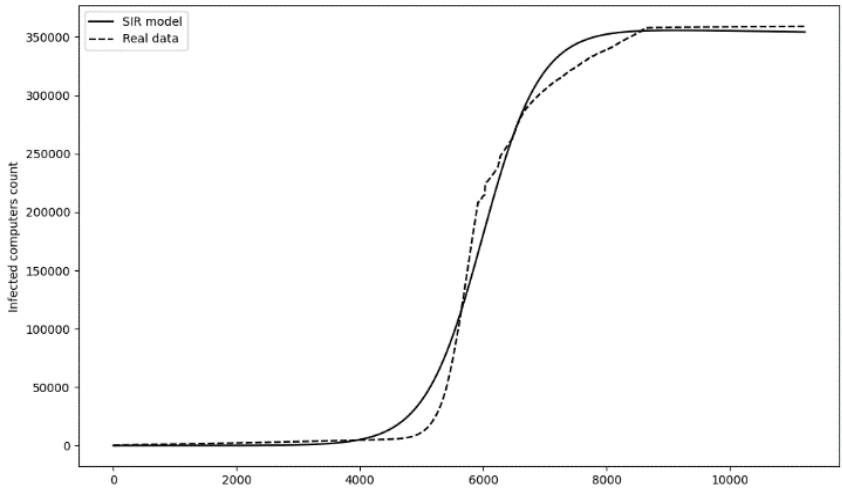


Figure 1 – SIR model of the worm propagation (solid), and the Code Red worm real data (dashed)

There can be many extensions to the SIR model, like the SIRA model [7, 8] with additional states for hosts secured by antivirus, etc. Although all these models fail to capture uncertainties such as:

– variability in user behavior, patching delay and accidental malware execution.

– network disruptions and architecture complexity.

– Responses to malware infections, such as patching or deploying anti-malware tools, are often delayed or irregular, introducing uncertainty in how quickly infections are mitigated.

These complexities necessitate stochastic models incorporating random variables into the modeling process, providing a more accurate and comprehensive representation of malware propagation.

Stochastic differential equations for the SIR epidemic model follow from a diffusion process. We add stochastic terms to the previous model to introduce randomness. In the SDE version, the equations are:

$$\begin{cases} \frac{dS}{dt} = -\beta IS + \sigma_S S dW(t), \\ \frac{dI}{dt} = \beta IS - \gamma I + \sigma_I S dW(t), \\ \frac{dR}{dt} = \gamma I. \end{cases}$$

where: s_S, s_I are the noise intensities affecting the susceptible and infected host numbers; $dW_S(t)$ and $dW_I(t)$ are the Wiener processes (random fluctuations).

Euler-Maruyama method [9] for stochastic differential equations is used to solve the model (see Figure 2 for the results).

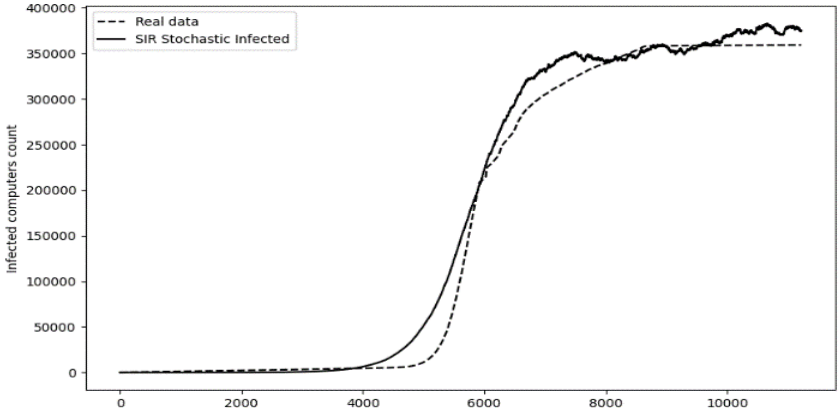


Figure 2 – SIR stochastic model of the worm propagation (solid), and the Code Red worm real data (dashed)

In this research, we explored deterministic and stochastic approaches to modeling the propagation of computer malware, with the Code Red worm serving as a primary case study. Initial approach models like SIR can be used to understand the worm propagation characteristics and estimate the need for mitigation approaches.

Conclusions. Stochastic models provide a more accurate and nuanced understanding of malware dynamics due to the incorporation of variable user behavior, network delays, and irregular system responses.

Future work can focus on extending models to more complex network architectures and incorporating real-time data from ongoing malware incidents for continuous model refinement.

Information sources

1. Kephart J. O. and White S. R. Directed-graph epidemiological models of computer viruses. In Proc. of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California, 1991, pp. 343–359. doi: 10.1109/RISP.1991. 130801.

2. Chumachenko D., Chumachenko K. and Yakovlev S. Intelligent simulation of network worm propagation using the code red as an example. Telecomm. Radio. Eng. 2019, 78(5), pp. 443–464. doi: 10.1615/TelecomRadEng.v78.i5.60.

3. Babasola O, Omondi E. O, Oshinubi K, Imbusi N. M. Stochastic Delay Differential Equations: A Comprehensive Approach for Understanding Biosystems with Application to Disease Modelling. AppliedMath. 2023, 3(4), pp. 702–721. doi: 10.3390/appliedmath3040037.

4. Semenyuk S. A., Chabanyuk Y. M. Stochastic evolution system with Markov-modulated Poisson perturbations in the averaging schema. Mat. Stud., 2024, 62(1), pp. 102–108. doi: 10.30970/ms.62.1.102-108.

5. CAIDA. “Code Red worm dataset” 20 Aug. 2001, [Online]. Available. URL: https://catalog.caida.org/dataset/telescope_codered_worm.

6. Harko T, Lobo F. S, Mak M. K. Exact analytical solutions of the Susceptible-Infected-Recovered (SIR) epidemic model and of the SIR model with equal death and birth rates, Appl. Math. and Comput. 2014, p. 236, pp. 184–194. doi: 10.1016/j.amc.2014.03.030.

7. Piqueira J. R. C., Navarro B. F., Monteiro L. H. A. Epidemiological models applied to viruses in computer networks. J. Comput. Sci. 1(1), pp. 31–34, 2005.

8. Amador J. The stochastic SIRA model for computer viruses, App. Math. and Comput. 2014, p. 232, pp. 112–124. doi: 10.1016/j.amc.2014.01.125.

9. Bayram M., Partal T. & Orucova Buyukoz G. Numerical methods for simulation of stochastic differential equations, Adv. Differ. Equ., 17, 2018. doi:10.1186/s13662-018-1466-5.

УДК 532.5.6

ІДЕНТИФІКАЦІЯ НЕПЕРЕВНИХ АКУСТИЧНИХ СИГНАЛІВ МАТЕМАТИЧНИМИ МЕТОДАМИ ДИСКРЕТИЗАЦІЇ ІНТЕГРАЛЬНИМИ ПЕРЕТВОРЕННЯМИ

Тарас ГЕМБАРА

Кафедра прикладної математики і механіки Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *An algorithm for processing reflected acoustic signals in buildings has been developed for object recognition technology against noise interference. The considered mathematical model takes into account that the input data (acoustic signals) are continuous functions of time with amplitude-frequency characteristics. To build the acoustic signal processing technology, signal discretization by integral transformations is used.*

Key words: *acoustic signal, amplitude-frequency response, integral Fourier transform, discretization.*

Анотація*. Розроблено алгоритм обробки відбитого акустичного сигналу в спорудах для технології розпізнавання об’єктів на фоні шумових перешкод. Розглянута математична модель враховує, що вхідні дані (акустичні сигнали) є неперервними функціями часу з амплітудно-частотними характеристиками. Для побудови технології обробки акустичного сигналу використовується дискретизація сигналів за інтегральними перетвореннями.*

Ключові слова: *акустичний сигнал, амплітудно-частотна характеристика, інтегральне перетворення Фур’є, дискретизація.*

Під час ліквідації наслідків бойових дій, зокрема наслідків ракетно-артилерійських ударів по будівлях, першочерговим завданням є пошук постраждалих в зруйнованих конструкціях. Постраждалі зазвичай подають сигнали про допомогу, як звукові (акустичні) в повітряному середовищі, так і ударні по ближнім елементам конструкцій. Тому актуальною задачею є ре-

єстрація, ідентифікація та верифікація таких сигналів, що має на меті встановлення (уточнення) місцезнаходження постраждалих. Основними завданнями для вирішення цієї задачі є розробка мобільних технічних засобів реєстрації акустичних сигналів в амплітудно-частотному часовому діапазоні та верифікація зареєстрованих амплітуд і частот у фіксовані моменти часу а також їх математична обробка за допомогою інтегральних перетворень та відповідного програмного забезпечення [1].

Акустичні хвилі, що розповсюджуються в будівлях, поділяються на повітряні та ударні. При повітряній передачі джерело звуку призводить до коливального руху частинок повітря, які передають періодичні коливання стіні або перекриттю (огородженню), змушуючи частинки матеріалу цих перешкод коливатися, що у свою чергу викликає коливання повітря в сусідньому приміщенні. Це створює повітряний акустичний сигнал у сусідньому приміщенні. При механічному (ударному) впливі на перешкоду, остання переходить у коливальний рух (згинальні коливання) і передає коливальний рух частинкам повітря. Крім того, коливання передаються частинам стін, що лежать зверху і знизу, і сприймаються у вигляді повітряного акустичного сигналу в сусідніх приміщеннях. Шляхи передачі акустичних хвиль в ізольоване приміщення можуть бути прямими і обхідними (непряме поширення акустичних хвиль).

Така передача пояснюється тим, що коливання, спричинені повітряним або ударним шумом, поширюються по конструкціях усієї будівлі. Для реєстрації акустичних сигналів використано вимірювач сигналів акустичної емісії BENETECH GM1356, який за рахунок високочутливого сенсора здатний реєструвати акустичні сигнали в діапазоні частот (від 31,5 Гц до 8,5 кГц) з високою точністю (± 1,5 дБ) з рівнем від 30 до 130 дБ, обладнаний функцією відтворення пікових значень на дисплеї та керування функцією автоматичного вимкнення живлення для тривалих вимірювань і моніторингу. До особливостей GM1356 належать: вибір типу фільтрації A і C, де зважуючий фільтр “A” охоплює весь частотний діапазон людського слуху і форма кривої схожа на те, як орган слуху людини сприймає гучність звуків залежно від частоти, а зважуючий фільтр “C” призначений для оцінки пікових рівнів джерел акустичних сигналів. Вихід AC/DC аналогового перетворювача сигналу призначений для аналізу за допомогою зовнішніх пристроїв.

За потреби тривалої роботи приладу, для збереження енергії батареї, передбачений роз’єм для під’єднання зовнішнього джерела живлення DC 6 В. Також GM1356 обладнаний USB-інтерфейсом для передавання даних на комп’ютер. Підключення до ПК через USB забезпечує завантаження запису даних, аналіз вибірки даних у реальному часі. Цей пристрій відповідає необхідним стандартам IEC PUB 651 TYPE2 і ANSI S1.4 TYPE2.

При цифровій обробці акустичного сигналу, необхідно виконати його дискретизацію і квантування. При цьому найважливішим завданням є об-

ґрунтований вибір частоти дискретизації. Від частоти дискретизації залежить спектр дискретного сигналу та його спотворення, пов'язані зі специфічними процесами, що виникають при дискретизації аналогового сигналу. Щодо дискретизації перевіряли виконання умов теореми Найквіста – Шеннона, фундаментального твердження в галузі цифрової обробки сигналів, що пов'язує неперервні і дискретні сигнали (рис. 1–2). Умови виконувались достатньо задовільно. Сигнал, отриманий пристроєм є аналоговим і аперіодичним. Тоді його спектр $S(\omega)$ визначається з використанням інтегрального перетворення Фур'є, де ω-частота коливань:

$$S(\omega) = \int_{-\infty}^{\infty} x(t)\, e^{-j\omega t} dt \qquad (1)$$

Скориставшись прямим перетворенням Фур'є, знайдемо спектр дискретного сигналу

$$S_Д(\omega) = \int_{-\infty}^{\infty} x(t)\, u(t)\, e^{-j\omega t}\, dt = U\frac{\tau}{T_Д}\int_{-\infty}^{\infty} x(t) \sum_{k=-K}^{K} e^{jk\omega_Д t} e^{-j\omega t} dt = \qquad (2)$$

$$= U\frac{\tau}{T_Д}\sum_{k=-K}^{K}\int_{-\infty}^{\infty} x(t)\, e^{-j(\omega - k\omega_Д)t} dt$$

Враховуючи (1), (2), отримаємо спектр дискретного сигналу виражений через спектр аналогового сигналу (рис. 1):

$$S_Д(\omega) = U\frac{\tau}{T_Д}\sum_{k=-K}^{K} S(\omega - k\omega_Д). \qquad (3)$$

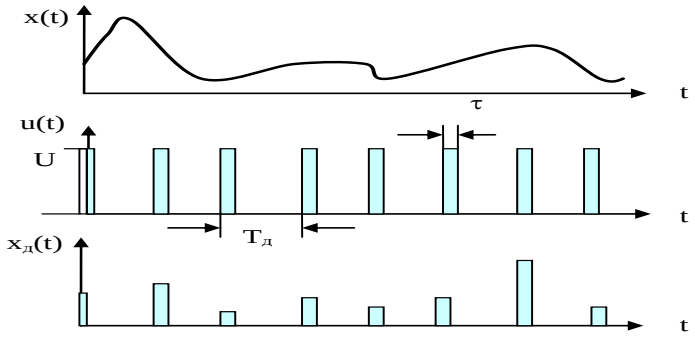


Рисунок 1 – Загальна схема накладення спектрів сигналів, $T_Д$–час дискретизації

Необхідні обчислення для спектрального моделювання і математичної обробки сигналів реалізовано в програмних пакетах Mathcad і Matlab. Задовільні результати отримано також при використанні замість (1) вейвлет-перетворення [1].

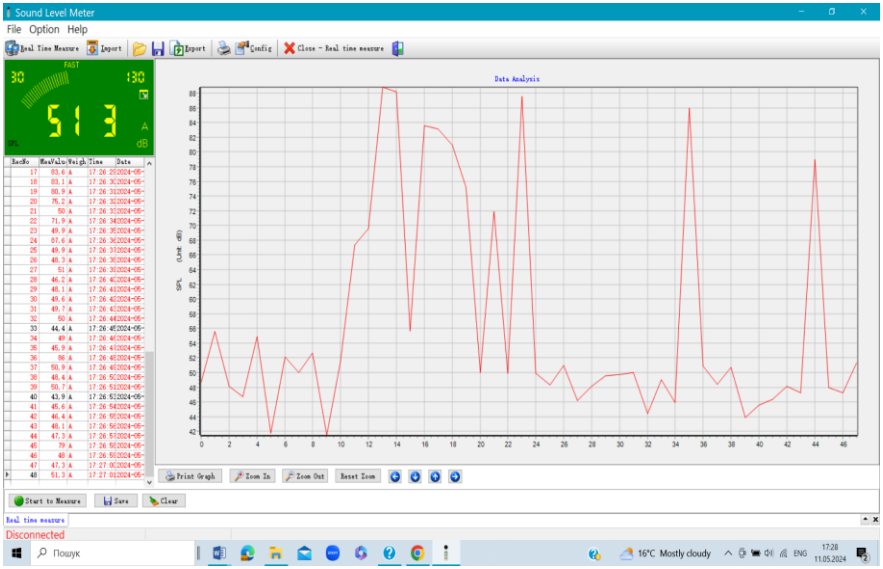


Рисунок 2 – Скріншот акустичних сигналів у режимі реального часу у максимальному діапазоні в дБ

Рисунок 3 – Скріншот акустичних сигналів в режимі реального часу на осцилографі

Для математичної обробки сигналів, отриманих через підключення вимірювача сигналів акустичної емісії до ПК через USB (рис. 2), використовувались сформовані файли дискретизації амплітудно-частотних даних програмою SoundLab (комплектується виробником пристрою). Одночасно відбувалась верифікація по каналу пристрою AC/DC на високоточному електронному осцилографі на моніторі ПК (рис. 3), у програмі Soundcard Oscilloscope.

Висновки. Встановлено, що перетворення Фур'є в класичному вигляді порівняно недостатньо забезпечують точність подання нестаціонарних сигналів, до яких належать мовні сигнали, де похибка становить 30–60%. В такому випадку спектрограми Вейвлет виявились перетворення набагато більш інформативні (похибка 20–40%), ніж звичайні Фур'є –спектрограми. Для сигналів ударної емісії точність ще вища, де похибка не перевищує 15%, а вибір інтегрального перетворення значення не має.

Інформаційні джерела

1. Дідковський В. С., Дідковська М. В., Продеус А. М. Комп'ютерна обробка акустичних сигналів. Навчальний посібник. – К.: "Імекс-ЛТД", 2010. – 420 с.

УДК 004.94.

РОЗРОБКА ПРОГРАМНОГО СЕРВІСУ ВИЗНАЧЕННЯ РІВНЯ ЗАБРУДНЕНЬ ПОВІТРЯ НА ДІЛЯНЦІ ДОРОГИ

Анастасія ІЛЬКІВ
Юрій БОРЗОВ

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *In the paper, the problems of environmental damage are considered, and the factors of road damage caused by the age of automobile transport are analyzed. A methodology for determining the level of emissions was proposed and a service was developed for determining safe impurities on a road section using an object-oriented programming language.*

Keywords: *motor vehicles, harmful impurities, service, software, interface, UML-diagram.*

Анотація. *В роботі розглянуто проблеми забруднення навколишнього середовища, проведено аналіз факторів забруднення автошляхів викидами автомобільного транспорту. Було запропоновано методику для визначення рівня викидів та розроблено сервіс для визначення кількості шкідливих домішок на ділянці дороги з використанням обє'ктно-орієнтованої мови програмування.*

Ключові слова: *автотранспорт, шкідливі домішки, сервіс, програмне забезпечення, інтерфейс, UML-діаграма.*

Стан навколишнього середовища в Україні має тенденцію до погіршення кожного року. Зміна клімату, погіршення якості повітря, води, ґрунту стають глобальними проблемами для України.

Автотранспорт є вагомим джерелом забруднення довкілля. В даний час на частку автомобільного транспорту припадає більше половини усіх шкідливих викидів у навколишнє середовище, які є головним джерелом забруднення атмосфери, особливо у великих містах. У середньому при пробігу 15 тис. км за рік кожен автомобіль спалює 2 т. палива і близько 26 – 30 т повітря, у тому числі 4,5 т кисню, що в 50 разів більше потреб людини. При цьому автомобіль викидає в атмосферу: чадного газу – 700 кг/рік, діоксиду азоту – 40 кг/рік, незгорілих вуглеводнів – 230 кг/рік і твердих речовин – 2 – 5 кг/рік.

Автомобільний транспорт забруднює атмосферу трьома способами: емісією шкідливих речовин з відпрацьованими газами, проривом газів у картер двигуна й емісією шкідливих речовин у результаті випару палива в паливних баках, карбюраторах, а також у результаті витоків палива. Головним з них є перший спосіб, на частку якого приходиться близько 2/3 шкідливих викидів автомобілів в атмосферу.

В ролі основних забруднювачів ґрунтів виступають метали та їхні сполуки. Масовий небезпечний характер носить забруднення ґрунтів свинцем. З'єднання свинцю використовують як добавку до бензину, тому автотранспорт є серйозним джерелом свинцевого забруднення.

Аналіз заходів із зниженням токсичності відпрацьованих газів автомобілів дозволяє виділити такі основні напрями боротьби зі шкідливим впливом автотранспорту на довкілля:

– використання нових типів силового устаткування з мінімальним викидом шкідливих речовин;

– заміна і вдосконалення конструкції, робочих процесів, технології виробництва автомобілів з метою зниження токсичності відпрацьованих газів;

– застосування пристроїв очищення або нейтралізації відпрацьованих газів (для автомобілів з бензиновими двигунами дуже ефективні каталітичні нейтралізатори потрійної дії, для дизельних автомобілів застосовують фільтри, які очищають відпрацьовані гази від сажі);

– використання альтернативного або зміна характеристик традиційного палива.

Отже, для зменшення негативного впливу складових частин транспортних комплексів на навколишнє природне середовище в Україні перш за все необхідно:

– впровадити жорсткий контроль за дотриманням допустимих норм викидів в атмосферне повітря;

– встановити контроль за дотриманням екологічних норм при побудові та експлуатації транспортної інфраструктури;

– проводити постійний контроль за технічним станом автомобілів;

– вдосконалити конструкції паливної системи двигуна;

– використовувати більш якісні паливно-мастильні речовини, що мають меншу концентрацію домішок.

Існує безліч методів прогнозування розповсюдження і трансформації забруднювальних речовин у повітрі. Було використано методику ОНД-86 для розрахунку максимальної приземної концентрації домішки у повітряному середовищі.

Методика розрахунку ОНД-86 найбільш підходить для вирішення поставлених у задач, оскільки дозволяє розраховувати концентрації шкідливих та будь-яких інших домішок у складі димових газів у двохметровому шарі над рівнем землі. Даний метод враховує:

– висоту труби;

– діаметр труби;

– витрати аналізованої речовини в атмосферу;

– температуру газів, що виходять із труби;

– перерізі труби;

– повні витрати димових газів на середню за перерізом труби швидкість газів;

– розсіювальні властивості атмосфери (кліматичний коефіцієнт);

– інтенсивність сепарації частинок (відношення швидкості осідання частинки до турбулентності, яка пропорційна швидкості вітру);

– метеорологічні дані (температуру навколишнього середовища, швидкість вітру);

– вплив рельєфу.

Дана методика може використовуватися і для автомобільного транспорту. В якості точкового джерела виступає вихлопна труба. За середніми показниками діаметр труби становить близько 55 міліметрів (0,055 метрів), а висота становить близько 365 міліметрів (0,365 метрів).

Розроблений програмний сервіс дозволяє визначати кількість шкідливих домішок на певній ділянці дороги. Для програмного коду була використана формула визначення максимальної концентрації забруднювальної речовини у приземному шарі атмосфери, що створюється одиночним точковим джерелом. Оскільки вихлопні гази є гарячими викидами, була використана відповідна формула:

$$C(\max) = \frac{MANnmh}{H^2 \sqrt[3]{V\Delta T}} \qquad (1)$$

Програмний код для сервісу визначення кількості шкідливих домішок на ділянці дороги було написано мовою програмування Java у середовищі ntelliJ IDEA, а інтерфейс створено за допомогою JavaFX Scenebuilder (рис. 1).

Сервіс аналізує введені дані з клавіатури і виводить кінцевий результат. У програмі є можливість порівняння результатів при зміні показників. Планується можливість перегляду графіків, що відображають результат.

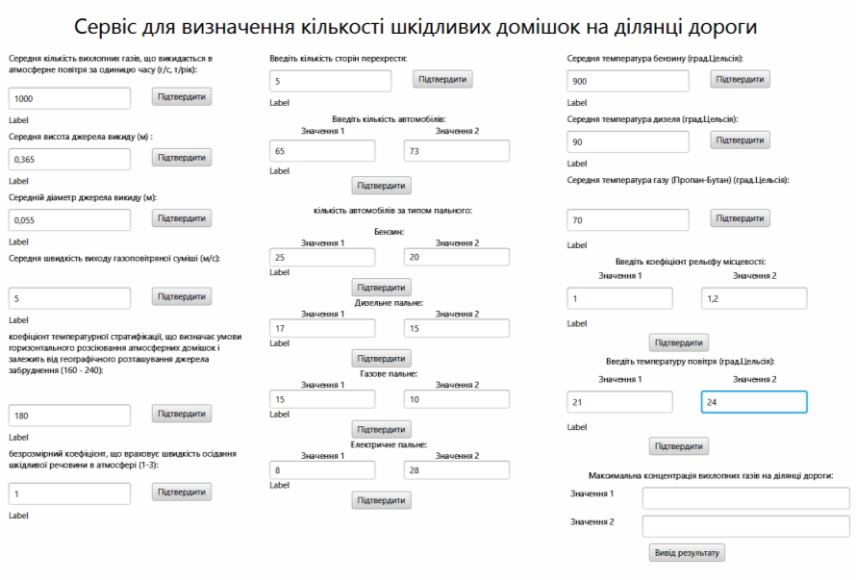


Рисунок 1 – Демо-версія інтерфейсу програмного забезпечення

Для розроблюваного сервісу було проведено моделювання з використанням UML-діаграм за допомогою середовища Visual Paradigm. Для представлення дій користувача приведено діаграму послідовності (рис. 2).

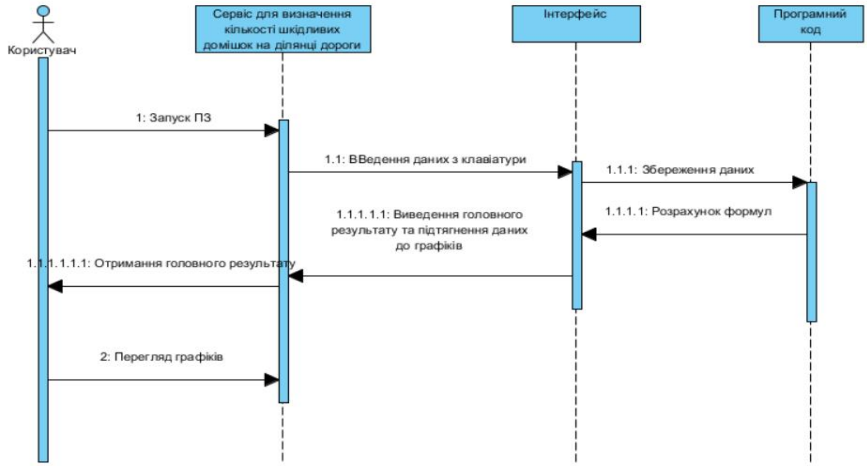


Рисунок 2 – Діаграма послідовності для введення даних
у програмному забезпеченні

Висновки. Запропонований сервіс визначення кількості шкідливих допоможе визначити та порівняти кількість шкідливих домішок на ділянці дороги і завдяки цьому здійснити заходи для покращення стану довкілля. Запрограмована методика дозволить прогнозувати стан забруднення на певній ділянці дороги з врахуванням завантаженості автотранспортом.

Інформаційні джерела

1. Закон України "Про основні засади (стратегію) державної екологічної політики України на період до 2020 року" від 21 грудня 2011 р. №2818-VI// Відомості Верховної Ради України. – 2011. – №26. – С. 218. URL: https://www.jetbrains.com/help/idea/opening-fxml-files-in-javafx-scene-builder. html

3. Про затвердження Порядку визначення величин фонових концентрацій забруднювальних речовин в атмосферному повітрі. Наказ Міністерства захисту довкілля та природних ресурсів № 599 від 17.09.2021.

УДК 004.94:655

СЕМАНТИЧНА МЕРЕЖА ФАКТОРІВ ВПЛИВУ НА ЯКІСТЬ ОБРОБЛЕННЯ КНИЖКОВИХ БЛОКІВ

Альона КУДРЯШОВА
Володимир ПЕТРИК
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *The process of book block processing has been studied with the aim of enhancing its strength, durability, and aesthetic appeal. Special attention has been paid to the influence of various processing stages on the quality of the final product, including gluing, drying, pressing, trimming, and finishing. Based on the analysis of these stages, a semantic network has been developed to reflect the interconnections among factors that determine the quality of book block processing. The developed network can be used for modeling influences and improving the efficiency of the technological process. The research methodology included expert evaluation, graph theory, and semantic networks to ensure a comprehensive approach to analyzing hierarchical relationships between processing stages.*

Keywords: *book block processing, semantic network, influencing factors, quality, technological process.*

Анотація. *Досліджено процес оброблення книжкових блоків з метою покращення їх міцності, довговічності та естетичної привабливості. Особливу увагу приділено впливу різних етапів обробки на якість кінцевого продукту, зокрема, заклеюванню, сушінню, обтискуванню, обрізуванню та оздобленню. На основі аналізу цих етапів розроблено семантичну мережу, яка відображає взаємозв'язки між факторами, що визначають якість оброблення книжкових блоків. Розроблена мережа може бути використана для моделювання впливів та покращення ефективності технологічного процесу. Методологія дослідження включала експертне оцінювання,*

теорію графів та семантичних мереж для забезпечення комплексного підходу до аналізу ієрархічних відносин між етапами оброблення.

Ключові слова: *оброблення книжкових блоків, семантична мережа, фактори впливу, якість, технологічний процес.*

Оброблення книжкових блоків є одним з ключових етапів післядрукарського опрацювання книжкових видань, що забезпечує отримання потрібного формату, підвищує міцність, довговічність та привабливість зовнішнього вигляду блоку. Цей процес включає низку операцій, які залежать від обраного варіанту оброблення книжкових блоків – зокрема, використовується шиття на марлі чи наклеювання марлі. Взаємозв'язок між операціями є критично важливим, оскільки кожен наступний етап базується на результатах попередніх. Таким чином, ефективне виконання кожного етапу забезпечує цілісність і довговічність книжкового блоку [1–3].

Метою дослідження є розроблення семантичної мережі факторів впливу на якість оброблення книжкових блоків. Для досягнення поставленої мети необхідно виконати такі завдання: виокремити та описати зв'язки між факторами впливу на якість оброблення книжкових блоків; розробити семантичну мережу у вигляді орієнтованого графу. Методи дослідження: експертне оцінювання для виокремлення факторів та зв'язків між ними; теорія графів та семантичних мереж.

При шитті на марлі обробка книжкового блоку проходить кілька основних етапів: заклеювання корінця для закріплення сторінок, сушіння корінця для підвищення міцності клею, обтискування для ущільнення та формування корінця, обрізування блоку з трьох сторін для надання акуратного вигляду, а також оздоблення обрізів, яке покращує естетику книги. Кожен із цих етапів сприяє покращенню загальних характеристик книжкового блоку, роблячи його більш надійним і зручним у користуванні, тому вважатимемо їх факторами впливу на якість оброблення книжкових блоків. Тоді множиною факторів впливу на якість досліджуваного процесу буде $X = \{x_1, x_2, x_3, x_4, x_5\}$, де x_1 – заклеювання корінця книжкового блоку, x_2 – сушіння корінця, x_3 – обтискування корінця, x_4 – обрізування блоку з трьох сторін, x_5 – оздоблення обрізів (рис. 1) [1, 4–6].

Заклеювання корінця книжкового блоку є фундаментальним етапом, що прямо або опосередковано впливає на всі наступні процеси оброблення. Якість заклеювання визначає надійність скріплення книжкового блоку, що безпосередньо впливає на його стійкість під час подальших операцій, таких як обтискування, обрізування та оздоблення.

Процес сушіння корінця залежить від попереднього етапу заклеювання. Тривалість та якість сушіння значною мірою впливають на стабільність та міцність блоку, а також забезпечують збереження його форми, що є критично

важливим для наступних процесів обтискування та обрізування. Належне висушування корінця запобігає його деформації під час подальшої обробки.

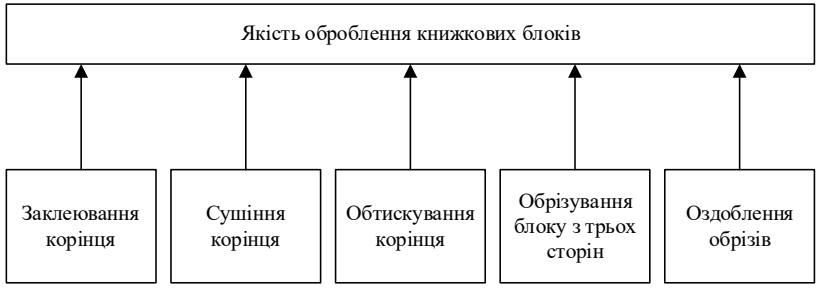


Рисунок 1 – Фактори впливу на якість оброблення книжкових блоків

Обтискування підвищує міцність корінця та створює оптимальні умови для рівномірного обрізування. Недостатнє обтискування може призвести до нерівностей на обрізах, що негативно позначиться на зовнішньому вигляді книжкового блоку.

Етап обрізування блоку з трьох сторін тісно пов'язаний з обтискуванням, оскільки лише коректно обтиснутий блок підлягає рівномірному обрізуванню. Нерівне обрізування здатне погіршити естетичний вигляд та якість подальшого оздоблення обрізів.

Оздоблення обрізів є завершальною стадією оброблення і залежить від якості виконання попередніх етапів, особливо обрізування. Належним чином підготовлені обрізи забезпечують рівномірність та естетичну привабливість оздоблення, що є важливим для створення якісного книжкового блоку [1].

Означимо впливи факторів:

- $x_1 - x_2$ – підготовлює;
- $x_1 - x_3$ – визначає міцність;
- $x_1 - x_4$ – підвищує точність;
- $x_2 - x_3$ – підвищує ефективність;
- $x_2 - x_4$ – забезпечує жорсткість;
- $x_3 - x_4$ – підвищує зручність;
- $x_3 - x_5$ – підготовлює;
- $x_4 - x_5$ – підготовлює.

На основі сформованих суджень розроблено семантичну мережу факторів впливу на якість оброблення книжкових блоків (рис. 2). Семантична мережа – це структура даних, яка використовується для представлення знань у вигляді графа, де вершини відповідають концептам або об'єктам, а ребра – зв'язкам між ними. Такий підхід дозволяє моделювати асоціації та ієрархічні

відносини між поняттями. Семантичні мережі застосовуються для представлення знань і логічних висновків [2, 7].

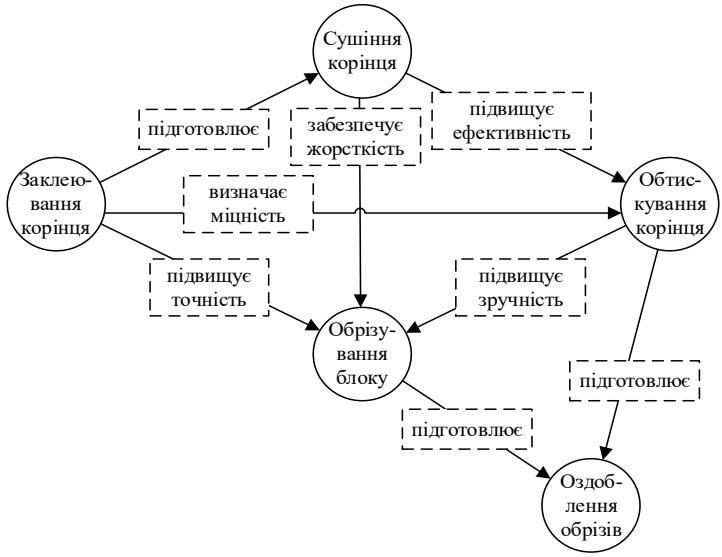


Рисунок 2 – Семантична мережа факторів впливу на якість оброблення книжкових блоків

Висновки. Результати дослідження підтвердили, що кожен етап оброблення книжкового блоку взаємопов'язаний і має критичний вплив на загальну якість готового продукту. Основними факторами впливу є якість заклеювання, яка визначає міцність книжкового блоку, належне сушіння корінця для забезпечення стабільності форми, а також обтискування, яке впливає на щільність і рівномірність обрізів. Обрізування і оздоблення, в свою чергу, завершують процес, забезпечуючи естетичний вигляд. Розроблена семантична мережа факторів впливу демонструє залежності між цими етапами, що дозволяє більш точно оцінювати та контролювати якість оброблення на кожному етапі. Застосування семантичної мережі як інструменту аналізу забезпечує можливість для подальшого удосконалення процесу виготовлення книжкових блоків, сприяючи підвищенню його ефективності та покращенню характеристик кінцевого продукту.

Інформаційні джерела

1. Маїк В. З. Технологія брошурувально-палітурних процесів : підр. / За заг. ред. д-ра. техн. наук, проф. Лазаренка Е. Т. Львів : УАД, 2011. 488 с.

2. Сеньківський В. М., Кудряшова А. В. Моделі інформаційної технології проєктування післядрукарських процесів: Монографія. Львів: УАД, 2022. 204 с.

3. Дурняк Б. В., Піх І. В., Сеньківський В. М. Теоретичні основи інформаційної концепції формування та оцінювання якості видавничо-поліграфічних процесів : Монографія. Львів: УАД, 2022. 356 с.

4. Senkivskyi V., Kudriashova A., Pikh I., Hileta I., Lytovchenko O. Models of Post-press Processes Designing. 1st International Workshop on Digital Content & Smart Multimedia, DCSMart 2019, Lviv, Ukraine, December 23–25, 2019, pp. 259–270.

5. Сеньківський В. М., Піх І. В., Кудряшова А. В. Теоретичні основи інформаційної технології прогностичного оцінювання якості проєктування післядрукарських процесів. New information technologies, simulation and automation: Monograph / Velychko V., Voinova S., Granyak V., et al; Editor-in-Chief Kotlyk S. Iowa State University Digital Press, 2022, 729 p. pp. 44–138.

6. Senkivskyi V., Kudriashova A., Pikh I., Hileta I., Lytovchenko O. Models of Postpress Processes Designing. 1st International Workshop on Digital Content & Smart Multimedia, DCSMart 2019, Lviv, Ukraine, December 23–25, 2019, pp. 259–270.

7. Senkivskyy V., Pikh I., Kudriashova A., Senkivska N., Tupychak L. Models of Factors of the Design Process of Reference and Encyclopedic Book Editions. In: Babichev S., Lytvynenko V. (eds) Lecture Notes in Computational Intelligence and Decision Making. ISDMCI 2021. Lecture Notes on Data Engineering and Communications Technologies, 2022, vol 77. Springer, Cham, pp. 217–229.

УДК 004.94:655

ОПТИМІЗАЦІЯ МЕТОДІВ ПОПЕРЕДНЬОЇ ОБРОБКИ ТА АУГМЕНТАЦІЇ ДАНИХ ДЛЯ НЕЙРОННИХ МЕРЕЖ У МЕДИЧНІЙ ВІЗУАЛІЗАЦІЇ ЛЕГЕНЬ

Ірина ПІХ
Назар МИХАЙЛЕВИЧ
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *Data preprocessing and augmentation methods for increasing the accuracy of neural networks in medical lung imaging have been investigated and optimized. Normalization, resizing, noise filtering and augmentation were used, which increased the accuracy of the models by 5–7%. An effective analysis methodology has been developed.*

Keywords: *data preprocessing, augmentation, neural networks, medical imaging, lungs.*

Анотація. *Досліджено та оптимізовано методи попередньої обробки і аугментації даних для підвищення точності нейронних мереж у медичній візуалізації легень. Використано нормалізацію, ресайзинг, фільтрацію шуму та аугментацію, що збільшило точність моделей на 5–7%. Розроблено ефективну методологію аналізу.*

Ключові слова: *попередня обробка даних, аугментація, нейронні мережі, медична візуалізація, легені.*

Медична візуалізація легень є важливим інструментом для діагностики захворювань, таких як пневмонія, туберкульоз та рак. Завдяки розвитку штуч-

ного інтелекту, зокрема глибоких нейронних мереж, автоматизований аналіз медичних зображень став можливим, що підвищує точність та ефективність діагностики. Проте, точність моделей залежить від якості та різновидів навчальних даних. Обмежена кількість доступних медичних зображень, високий рівень шуму та неналежні умови зйомки створюють серйозні виклики.

Основна проблема – недостатня кількість якісних даних, що призводить до перенавчання та зниження здатності моделей до узагальнення. Для подолання цих обмежень необхідно застосовувати методи попередньої обробки та аугментації, що покращують якість і мультиплікатність даних.

Метою дослідження є оптимізація методів попередньої обробки та аугментації даних для підвищення точності нейронних мереж у медичній візуалізації легень. Планується дослідити вплив різних технік на продуктивність моделей та розробити стратегії, що дозволять збільшити їх точність на 5–7%.

Попередня обробка даних включає кілька етапів, спрямованих на підвищення якості вхідних зображень та підготовку їх до навчання моделі:

1. *Нормалізація зображень*: Приведення значень пікселів до стандартного діапазону [0,1] для забезпечення стабільності навчання.

$$I_{normalized} = \frac{I - I_{\min}}{I_{\max} - I_{\min}} \qquad (1)$$

Нормалізація допомагає уникнути проблем зі швидкістю навчання та сприяє кращій конвергенції моделей [1].

2. *Ресайзинг*: Зміна розміру зображень до стандартних розмірів S, *наприклад*, 224 × 224 пікселів, відповідно до вимог архітектур CNN [2].

3. *Фільтрація шуму*: Використання гаусівського фільтра для зменшення шуму та покращення якості зображення.

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}} \qquad (2)$$

Фільтрація шуму дозволяє зменшити вплив артефактів на процес навчання моделі [3].

Аугментація даних дозволяє збільшити різноманітність навчальної вибірки за рахунок застосування різних трансформацій до вихідних зображень:

1. *Обертання*: Випадкове обертання зображення на кут від –30° до 30°.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \qquad (3)$$

Обертання допомагає моделі бути більш стійкою до орієнтації об’єктів на зображенні [4].

2. *Зсув*: Випадковий зсув зображення по горизонталі та вертикалі.

$$I_{shifted}(x,y) = I(x + \Delta x, y + \Delta y) \qquad (4)$$

Зсув забезпечує моделі можливість розпізнавання об'єктів у різних положеннях [4].

3. *Віддзеркалення*: Горизонтальне та вертикальне віддзеркалення зображення.

$$I_{flipped}(x,y) = I(-x,y) \text{ або } I(x,-y) \quad (5)$$

Віддзеркалення збільшує симетрію даних, що сприяє покращенню узагальнення моделей [5].

4. *Випадкова зміна яскравості*: Випадкова зміна яскравості та контрасту для імітації різних умов зйомки.

Зміна яскравості та контрасту описується наступними формулами:

$$I_{new}(x,y) = \alpha \cdot I(x,y) + \beta \quad (6)$$

де: α – коефіцієнт контрасту (зазвичай α>1 для збільшення контрасту; α<1 для зменшення); β – коефіцієнт яскравості (додається до кожного пікселя для зміни яскравості).

Ця техніка дозволяє моделі адаптуватися до різних освітлювальних умов, що часто зустрічаються в медичних зображеннях [5].

Для оптимізації методів попередньої обробки та аугментації даних використовувалися різні архітектури нейронних мереж, зокрема ResNet-50 та EfficientNet-B0. Архітектура ResNet-50 дозволяє глибоко навчати модель завдяки використанню залишкових з'єднань, що запобігає проблемі зникнення градієнта [5]. EfficientNet-B0 відзначається високою ефективністю та компактністю моделі, що дозволяє досягати високої точності при менших обчислювальних витратах [3].

Для оцінки ефективності оптимізованих методів попередньої обробки та аугментації використовувалися метрики точності (Accuracy), чутливості (Sensitivity) та специфічності (Specificity). Формули для розрахунку цих метрик наведені нижче:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (7)$$

$$Sensitivity = \frac{TP}{TP + FN} \quad (8)$$

$$Specificity = \frac{TN}{TN + FP} \quad (9)$$

де *TP* – кількість істинно позитивних результатів; *TN* – кількість істинно негативних результатів; *FP* – кількість хибно позитивних результатів; *FN* – кількість хибно негативних результатів [6].

Результати. Проведені експерименти показали, що оптимізовані методи попередньої обробки та аугментації даних значно підвищують продуктивність

нейронних мереж у завданнях медичної візуалізації. Застосування методів аугментації дозволило збільшити точність моделей ResNet-50 та EfficientNet-B0 на 5–7% порівняно з базовими методами підготовки даних (рис. 1).

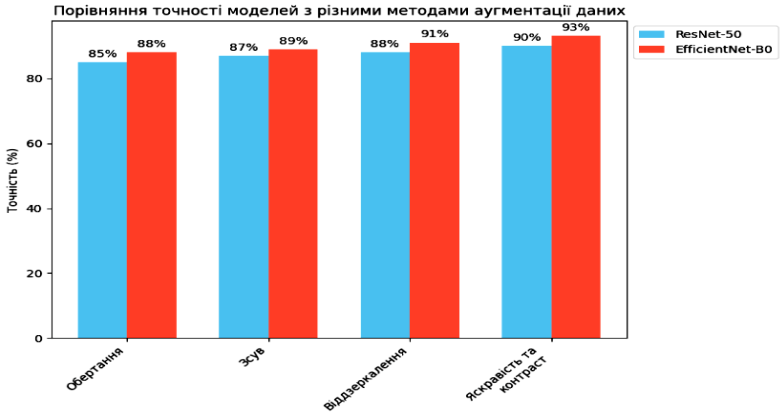


Рисунок 1 – Порівняння точності моделей з різними методами аугментації даних

На графіку наведено порівняння точності моделей ResNet-50 та EfficientNet-B0 при використанні різних методів аугментації даних. На осі X позначені різні методи аугментації (Обертання, Зсув, Віддзеркалення, Яскравість та контраст), а на осі Y – відповідна точність моделей у відсотках. Видно, що комбінація методів аугментації призводить до найбільшого зростання точності обох моделей.

Результати дослідження свідчать про важливість оптимізації методів попередньої обробки та аугментації даних для підвищення ефективності нейронних мереж у медичній візуалізації. Збільшення різноманітності навчальної вибірки за рахунок аугментації дозволяє моделям краще узагальнювати знання та знижує ризик перенавчання. Особливо ефективним виявився метод зміни яскравості та контрасту, що дозволив моделі краще справлятися з різними умовами зйомки. Це підтверджується іншими дослідженнями, де аналогічні методи аугментації також показали позитивний вплив на продуктивність моделей [1, 2, 4].

Висновки. Оптимізація методів попередньої обробки та аугментації даних є критично важливим етапом у підготовці навчальної вибірки для нейронних мереж у медичній візуалізації. Проведене дослідження показало, що застосування різних методів аугментації значно підвищує точність моделей, таких як ResNet-50 та EfficientNet-B0. Подальші дослідження можуть бути спрямовані на інтеграцію складніших методів аугментації та визначення їх впливу на архітектури нейронних мереж.

Інформаційні джерела

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. The MIT Press, 2016, 800 p.
2. Shorten C., Khoshgoftaar T. M. A survey on Image Data Augmentation for Deep Learning. Journal of Big Data, 2019, Vol. 6, No. 1, pp. 1–48.
3. Tan M., Le Q. V. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. International Conference on Machine Learning (ICML), 2019, pp. 6105–6114.
4. Krizhevsky A., Sutskever I., Hinton G. E. ImageNet Classification with Deep Convolutional Neural Networks. Advances in Neural Information Processing Systems (NeurIPS), 2012, pp. 1097–1105.
5. He K., Zhang X., Ren S., Sun J. Deep Residual Learning for Image Recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 770–778.
6. Powers D.M.W. Evaluation: from Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation. Journal of Machine Learning Technologies, 2011, Vol. 2, No. 1, pp. 37–63.

УДК 004.432.4

МОДЕЛЬНО-ОРІЄНТОВАНИЙ ПІДХІД ДО АВТОМАТИЗАЦІЇ ГЕНЕРАЦІЇ ТЕСТОВИХ ВИПАДКІВ НА ОСНОВІ UML ДІАГРАМ

Марта ЛІННИК
Юлія НАЗАР

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *This paper describes an approach to automating the process of generating test cases based on UML models. Various UML diagrams are considered for test generation, including Use Case Diagram, Class Diagram, Sequence Diagram, Use Case templates, and a data dictionary expressed in OCL. The methodology ensures automation of the testing process without significant modifications to the initial models.*

Keywords: *UML models, class diagram, position diagram, test-cases, test process.*

Анотація. *В даній роботі описано підхід до автоматизації процесу генерації тест-кейсів на основі UML моделей. Для генерації тестів розглядаються різні UML діаграми, зокрема діаграма варіантів використання, діаграма класів, діаграма послідовностей, шаблони варіантів використання та словник даних, виражений в OCL. Методологія забезпечує автоматизацію процесу тестування без складних змін у початкових моделях.*

Ключові слова: *UML діаграми, діаграма класів, діаграма послідовностей, тест-кейси, процес тестування.*

Відомо, що традиційне тестування зазвичай створює тестові сценарії, ґрунтуючись на вихідному коді програми. Для цього програму перетворюють у різні високорівневі моделі, такі як діаграми керування потоком,

графи потоків даних або графи викликів. Загалом це називається тестуванням на основі моделей. Простими словами – це техніка тестування програмного забезпечення, за якої поведінка тестованого програмного забезпечення під час виконання перевіряється на прогнози, зроблені моделлю, де модель – це опис поведінки системи. У такому підході тести створюються на основі абстрактних моделей програмного забезпечення, зокрема формальних специфікацій або UML-діаграм, які є напівформальними описами дизайну. Автоматична генерація тестових випадків із напряму з UI моделей має значні переваги. Процес створення тестів вручну є трудомістким і вимагає багато часу та ресурсів, тому автоматизація цього процесу дозволяє суттєво зменшити затрати, забезпечуючи швидке та ефективне тестування. Ще однією перевагою є те, що тест-кейси можна створювати на ранніх етапах розробки, ще до написання програмного коду. Це дає змогу розробникам використовувати готові тести під час створення коду, що зменшує кількість повторних перевірок і циклів між розробкою та тестуванням, додатково економлячи ресурси.

Unified Modeling Language (UML) стала універсальною мовою для моделювання програмних систем. Вона використовується для специфікації, візуалізації, побудови та документування різноманітних компонентів програмного забезпечення. Особливо корисними для тестування є діаграми послідовностей, які фіксують взаємодію між об'єктами у часі. Ці діаграми детально описують взаємодію між компонентами системи, що робить їх природним джерелом для інтеграційного тестування. Системне тестування часто вважається найскладнішим і найретельнішим видом тестування, оскільки воно охоплює всі аспекти функціонування системи.

Для створення тест-кейсів потрібно трансформувати діаграми варіантів використання (UD), діаграми класів (CD) та діаграми послідовностей (SD) у спеціальне представлення, яке називається графом діаграми послідовностей (SDG). Кожен вузол цього графа містить необхідну інформацію для генерації тест-кейсів. Ця інформація збирається з різних джерел: шаблону варіанта використання (також відомого як розширений варіант використання), діаграм класів і словника даних, представленого у вигляді обмежувальних виразів мовою OCL (Object Constraint Language). Наступним кроком є обхід графа SDG для створення тестових випадків відповідно до заданих критеріїв покриття та обраної моделі помилок. Схематична блок-діаграма такого підходу зображена на рисунку 1.

Для розуміння системи в цілому відбувається створення діаграми випадків використання, діаграми класів та діаграми послідовностей. UML-діаграми будуємо за допомогою інструменту Draw.io, оскільки цей інструмент має хорошу підтримку для виразів OCL та є більш зручним порівняно з іншими інструментами. Рисунок 2 представляє діаграму послідовностей для сайту для моніторингу повітряних тривог, зокрема для сценарію перегляду актуальних тривог та попереджень.

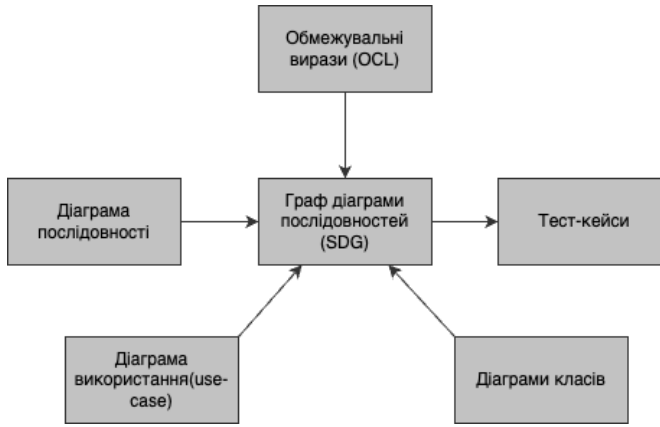


Рисунок 1 – Діаграма для запропонованого підходу

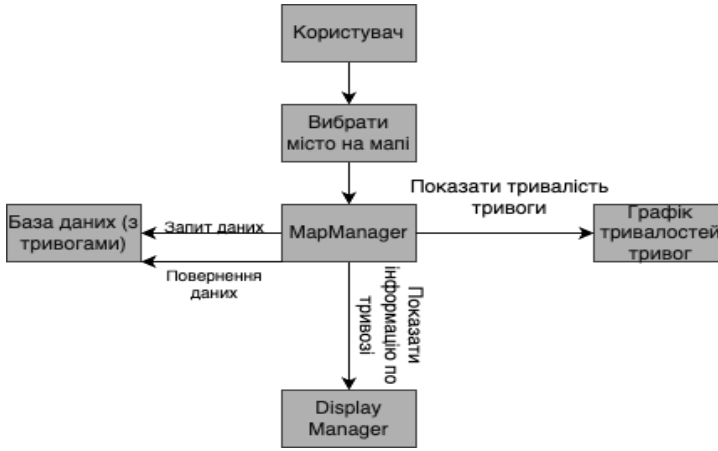


Рисунок 2 – Діаграма послідовностей для Мапи тривог

Парсер працює так, що він читає XML файл, експортований на попередньому етапі, та надає опис усіх тегів і атрибутів з цього файлу. Ця інформація є важливою для генерації опису діаграми послідовностей у вигляді графа, який містить вузли, що зберігають необхідну інформацію для створення сценаріїв. У проєкті використовується API на основі дерева, до прикладу Document Object Model (DOM), яке будує деревоподібну репрезентацію XML-документа в пам’яті. Це API надає класи та методи, які дозволяють програмі здійснювати навігацію та обробляти дерево, що є основою для подальшої обробки даних з XML файлу. Такий підхід дозволяє ефективно пра-

цювати з великими обсягами структурованої інформації та зберігати її у вигляді, зручному для подальшої генерації тестів або створення графів на основі UML-діаграм.

```
<stateX>
S1: null citySelected :MapManager :CitySelector uml:Message
S2: null requestAlertData :MapManager :AlertDatabase uml:Message
S3: null receiveAlertData :AlertDatabase :MapManager uml:Message
S4: null displayAlertInfo :MapManager :DisplayManager uml:Message
S5: null showAlertDuration :MapManager :DurationGraph uml:Message
context MapManager::displayAlertInfo(); pre: AlertDatabase.alerts="CityAlerts"; post: result="Display
city alert data including duration & chart" OCL2.0 uml:OpaqueExpression
<StateY>

<StateX>
S1: null mapOpened :MapManager :DisplayManager uml:Message
S2: null selectAlertType :MapManager :AlertSettingsManager uml:Message
S3: null displayAlertTypes :AlertSettingsManager :DisplayManager uml:Message
S4: null alertTypeSelected :AlertSettingsManager :MapManager uml:Message
S5: null updateAlertMap :MapManager :MapEditor uml:Message
context MapManager::updateAlertMap(); pre: AlertSettingsManager.alertType="SelectedType"; post:
result="Map updated with selected alert type" OCL2.0 uml:OpaqueExpression
S6: null alertTypeChanged :MapManager :AlertSettingsManager uml:Message
S7: null refreshMapDisplay :MapManager :DisplayManager uml:Message
<StateY>
```

Рисунок 3 – Вивід згенерованих сценаріїв

Графічне відображення вузлів, що йдуть від StateX до StateY зображене на рисунку 4. Спочатку відображаються всі вузли першого сценарію, після чого, можна по черзі обирати та бачити вузли решти сценаріїв. Цей підхід дозволяє користувачу наочно переглядати різні етапи виконання сценаріїв та зв’язок між різними вузлами, що представляють послідовність подій і дії системи.

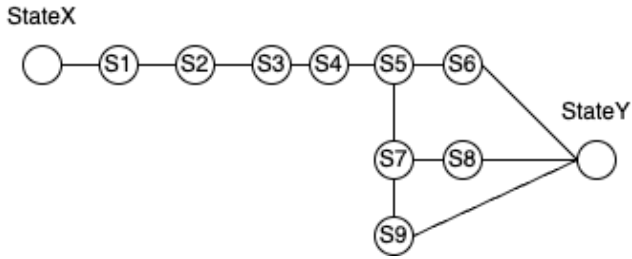


Рисунок 4 – Відображення графа діаграми послідовностей

Висновки. У результаті виконання даного дослідження розроблено модельно-орієнтований підхід для автоматизації генарації тестових випадків програмної системи із використанням UML діаграм. Представлено методологію перетворення UML діаграми послідовностей у граф послідовностей (SDG),

який слугує основою для подальшої автоматизації тестування. Запропонований підхід включає етапи аналізу та парсингу XML-файлів UML діаграм, побудову графа сценаріїв і використання цього графа для створення тестових випадків. Методологія забезпечує автоматичне виділення інформації про передумови, післяумови та повідомлення між об'єктами на основі OCL-виразів, що дозволяє генерувати тестові сценарії без необхідності внесення змін до початкових UML-моделей. Це значно скорочує час на розробку тестів, мінімізує людські помилки та сприяє підвищенню якості програмного забезпечення. Автоматизація на основі запропонованої методики дозволяє ефективніше реалізовувати процеси валідації та перевірки програмних систем, орієнтованих на безпеку або інші критично важливі області застосування.

Інформаційні джерела

1. Смотр О. О., Придатко О. В., Малець І. О. Основи програмування (Phyton, Java). Львів, 2019. – С. 28 – 74.

2. Коберник С. О., Тарасенко В. О. Моделювання процесів проектування програмного забезпечення на основі діаграм послідовностей UML. Вісник Національного університету "Львівська політехніка", серія "Інформатика, обчислювальна техніка та автоматизація", 2020, №15. – С. 82–90.

3. Хом'як В. О., Андрущенко О. В. Автоматизоване тестування програмних продуктів на основі поведінкових моделей. Інформаційні системи і технології в медицині, том 3, № 2, 2022. – С. 39, 47.

4. Мельник І. М., Копайгора О. В. Моделювання та автоматизоване тестування програмного забезпечення на основі графів. Вісник НТУ "ХПІ". Серія: Інформатика та моделювання, випуск 1, 2021. – С. 57–62.

УДК 004.942:681.625.23

МОДЕЛЮВАННЯ ТА АНАЛІЗ ПРОЦЕСУ ОФСЕТНОГО ДРУКУ

Михайло ВЕРХОЛА

Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *This paper proposes a computer technology for analyzing the ink transfer process in offset printing systems, which makes it possible to obtain information about the required parameters of the ink and wetting solution input before printing, which significantly reduces the time required to prepare offset machines for printing.*

Keywords: *inkjet printing system, offset printing, computer modulation, wetting solution, emulsified ink, simulator.*

Анотація. *В даній роботі пропонується комп'ютерна технологія аналізу процесу передачі фарби у фарбодрукарських системах офсетного типу, яка дає можливість отримувати інформацію про необхідні параметри вхідного завдання фарби і*

зволожувального розчину до початку друку, що суттєво скорочує затрати часу на підготовку офсетних машин до друку.

Ключові слова: *фарбодрукарська система, офсетний друк, комп'ютерне моделювання, зволожувальний розчин, емульгована фарба, симулятор.*

На ринку поліграфічних послуг офсетний друк є найбільш поширеним оскільки за його допомогою отримується близько 50% сучасної поліграфічної продукції. Він є ефективним при тиражуванні книг, журналів, етикеток та іншої продукції.

Принцип роботи фарбової підсистеми офсетної машини полягає у відокремленні від загального об'єму фарби, завантаженої у дукторну скриньку, шару фарби значно більшої товщини від потрібної для нанесення на друкарську форму. Після цього, товщина фарби в процесі передачі системою валиків і циліндрів зменшується до необхідної товщини і наноситься на поверхню форми. Процес підготовки фарбового шару послідовно здійснюється трьома групами: *фарбоживильною*, призначеною для відбору фарби з фарбової скриньки; *розкочувальною*, яка забезпечує створення рівномірного суцільного шару фарби на поверхні накочувальних валиків; *накочувальною*, що призначена для нанесення тонкого (1–2 мкм) рівномірного шару фарби на друкувальні елементи форми.

Зволожувальні підсистеми, за своєю конструкцією, подібні до спрощених фарбових підсистем, і їхнє призначення полягає в нанесенні контактним способом на поверхню друкарської форми рівномірного шару зволожувального розчину для підсилення контрастності друкувальних і пробільних елементів.

Особливістю офсетного друку є те, що друкувальні і пробільні елементи форми, які відтворюють зображення, розміщені в одній площині, тому для отримання якісних відбитків на поверхню форми необхідно одночасно подавати фарбу і зволожувальний розчин та підтримувати баланс цих двох композиційних рідин в процесі друку [1].

Необхідний баланс фарби і розчину налагоджується під час підготовки офсетної машини до друку на основі досвіду і кваліфікації друкаря та вимагає відповідних затрат часу, паперу і фарби.

Підвищення ефективності офсетного друку, в умовах конкуренції з цифровим, вимагає ґрунтовних досліджень. Експериментальні дослідження не дають бажаного результату через відсутність необхідної високоточної вимірювальної апаратури та вплив технологічних збурень, які генеруються під час роботи офсетної машини.

В даній роботі пропонується комп'ютерна технологія аналізу процесу розподілу і передачі фарби та зволожувального розчину у фарбодрукарських системах офсетного типу.

Методику розроблення такої технології продемонстровано *на прикладі* однопотокової фарбодрукарської системи з розтиральними циліндрами, сигнальний граф якої представлено на рисунку 1.

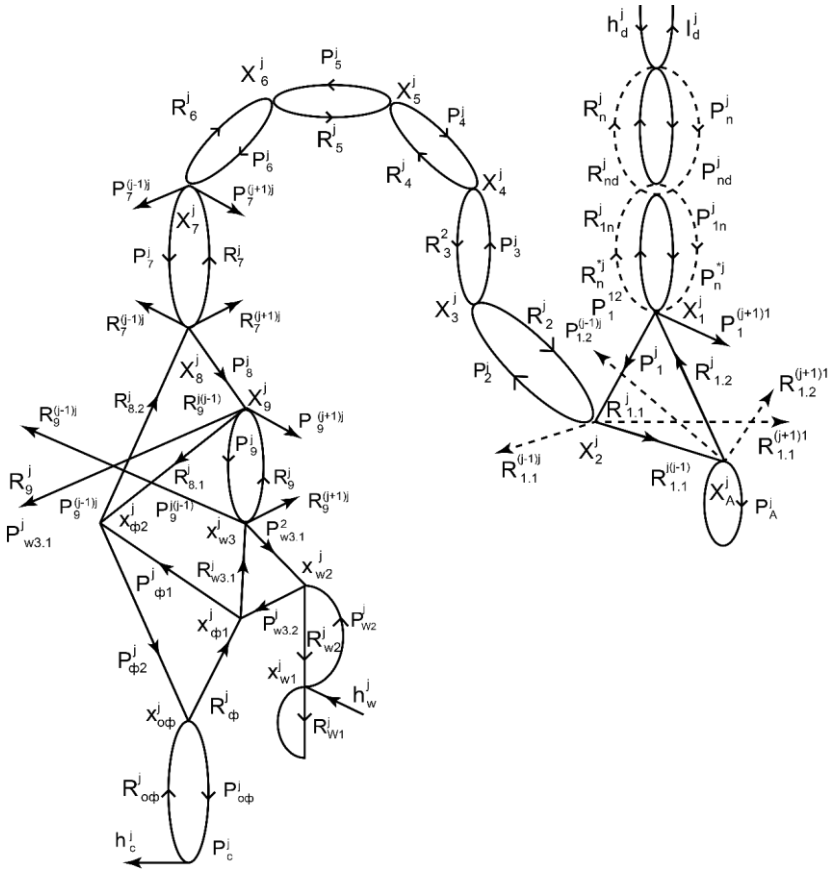


Рисунок 1 – Сигнальний граф j-тої зони фарбодрукарської системи

Сигнальний граф описує зв’язки між змінними та складається з вузлів (вершин) і віток, що їх з’єднують. Вітки відображають залежності між змінними, а вершини графа – товщини потоків фарби, що сумуються в місцях контакту суміжних валиків і циліндрів.

Дуги графа візуалізують оператори руху прямих і зворотних мікропотоків фарби в j-тих зонах поверхонь елементів фарбодрукарської системи. Відрізки направлені в сторони суміжних зон графа візуалізують переміщення прямих і зворотних потоків фарби розтиральними циліндрами в осьовому напрямі. Вхідні вершини графа відповідають зональним потокам фарби на поверхні дуктора а вихідні товщинам фарби, що передається у відповідні зони відбитків.

$$ex_n^j(z) = P_{1n}^j(z)P_n^j(z)ex_n^j(z) + P_n^{*j}(z)P_{dn}^j(z)ex_n^j(z) +$$
$$+R_{1.2}^{j(j-1)}(z)ex_A^j(z) + R_{1.2}^j(z)ex_A^j(z) + R_{1.2}^{j(j+1)}(z)ex_A^j(z);$$
$$ex_2^j(z) = P_1^{j(j-1)}(z)ex_1^{j(j-1)}(z) + P_1^j(z)ex_1^j(z) + P_1^{j(j+1)}(z)ex_1^{j(j+1)}(z) + R_2^j(z)ex_3^j(z);$$
$$ex_A^j(z) = R_{1.1}^{j(j-1)}(z)ex_2^{j(j-1)}(z) + R_{1.1}^j(z)ex_2^j(z) + R_{1.1}^{j(j+1)}(z)ex_2^{j(j+1)}(z) + P_A^j(z)ex_A^j(z);$$
$$ex_3^j(z) = P_2^j(z)ex_2^j(z) + R_3^j(z)ex_4^j(z);$$
$$ex_4^j(z) = P_3^j(z)ex_3^j(z) + R_4^j(z)ex_5^j(z);$$
$$ex_5^j(z) = P_4^j(z)ex_4^j(z) + R_5^j(z)ex_6^j(z);$$
$$ex_6^j(z) = P_5^j(z)ex_5^j(z) + R_6^j(z)ex_7^j(z);$$
$$ex_7^j(z) = P_6^j(z)ex_6^j(z) + R_7^{j(j-1)}(z)ex_9^{j(j-1)}(z) + R_7^j(z)ex_9^j(z) + R_7^{j(j+1)}(z)ex_9^{j(j+1)}(z);$$
$$ex_8^j(z) = P_7^j(z)ex_7^j(z) + P_7^{j(j-1)}(z)ex_7^{j(j-1)}(z) + R_7^{j(j+1)}(z)ex_7^{j(j+1)}(z) + R_8^j(z)ex_\phi^j(z);$$
$$ex_9^j(z) = P_{8.1}^j(z)ex_8^j(z) + P_9^{j(j-1)}(z)ex_{w2}^{j(j-1)}(z) + P_9^j(z)ex_{w3}^j(z) + P_9^{j(j+1)}(z)ex_{w3}^{j(j+1)}(z);$$
$$ex_{w1}^j(z) = F_w(z)(R_{w2}^j(z)(ex_{w2}^j(z) - (1+k_e)x_{w2}^j(z)) + R_{w1}^j(z)(ex_{w1}^j(z) - (1+k_e)x_{w1}^j(z)) + rh_d^j(z);$$
$$ex_{w2}^j(z) = R_{w3.2}^j(z)ex_9^j(z) + P_{w2}^j(z)ex_{w1}^j(z);$$
$$ex_{w3}^j(z) = R_9^{j(j-1)}(z)ex_9^{j(j-1)}(z) + R_9^j(z)ex_9^j(z) + R_9^{j(j+1)}(z)ex_9^{j(j+1)}(z) + R_{w3.1}^j(z)ex_{\phi 1}^j(z);$$
$$rx_{\phi 1}^j(z) = P_{w3}^j(z)rx_{w2}^j(z) - (1+k_e)P_w^j(z)x_{w2}^j(z) + R_\phi^j(z)rx_{o\phi}^j(z);$$
$$ex_{\phi 1}^j(z) = (1+k_e)P_{w3}^j(z)x_{w2}^j(z) + R_\phi^j(z)ex_{o\phi}^j(z);$$
$$rx_{\phi 2}^j(z) = P_{8.2}^j(z)rx_9^j(z) - (1+k_e)R_{8.2}^j(z)x_9^j(z)) + F_{П1}^j P_{\phi 1}^j(z)rx_{\phi 1}^j(z);$$
$$ex_{\phi 2}^j(z) = (1+k_e)P_{8.2}^j(z)x_9^j(z) + F_{Д1}^j P_{\phi 1}^j(z)ex_{\phi 1}^j(z);$$
$$rx_{o\phi}^j(z) = F_{П3}^j P_{\phi 3}^j(z)rx_{\phi 3}^j(z) + R_{o\phi}^j(z)rx_c^j(z);$$
$$ex_{o\phi}^j(z) = F_{Д3}^j P_{\phi 3}^j(z)ex_{\phi 3}^j(z) + R_{o\phi}^j(z)ex_c^j(z);$$
$$rx_c^j(z) = P_{o\phi}^j(z)rx_{o\phi}^j(z);$$
$$ex_c^j(z) = P_{o\phi}^j(z)ex_{o\phi}^j(z);$$
$$rh_c^j(z) = P_c^j(z)rx_c^j(z);\ eh_c^j(z) = P_c^j(z)ex_c^j(z), \qquad (1)$$

де $ex_n^j(z)$, $ex_1^j(z)$, $ex_2^j(z)$,…, $ex_9^j(z)$, $ex_{w1}^j(z)$, $ex_{wA}^j(z)$, $ex_{w2}^j(z)$ – товщини емульгованої фарби в j-тих зонах контакту елементів фарбової та зволожувальної підсистем, подані у z-зображеннях; $ex_{\phi 1}^j(z)$, $ex_{\phi 2}^j(z)$, $ex_{\phi 3}^j(z)$ – товщини емульгованої фарби та зволожувального розчину ($rx_{\phi 1}^j(z)$, $rx_{\phi 2}^j(z)$, $rx_{\phi 3}^j(z)$) в j-тих зонах контакту накочувальних валиків з формою; $eh_c^j(z)$, $rh_c^j(z)$ – товщини фарби та розчину *j*-тих зон відбитків.

На основі системи рівнянь (1) і сигнального графа (рис. 1) у середовищі Matlab Simulink побудовано симулятор фарбодрукарської системи, що включає фарбову, зволожувальну і друкарську підсистеми. Під час побудови симулятора враховуються: структура фарбодрукарської системи; довжини дуг валиків і циліндрів між точками їх контакту; композиція розміщення друкувальних елементів на поверхні форми; період подачі фарби та цикл роботи розтиральних циліндрів.

Проведено імітаційне моделювання та дослідження впливу коефіцієнтів розщеплення фарби у зонах контакту елементів фарбодрукарської системи на процес передачі фарби і зволожувального розчину від джерел їх подачі до відбитків.

Динаміку процесу передачі фарби і зволожувального розчину на матеріал, що задруковується показано на рисунку 2.

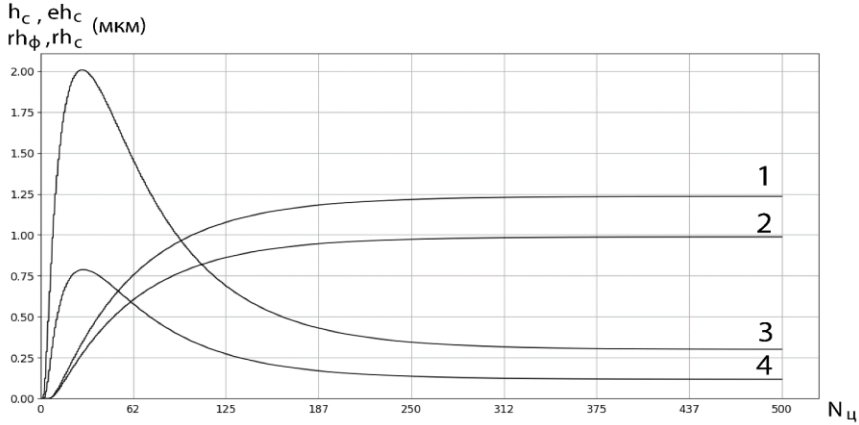


Рисунок 2 – Перехідні процеси товщин фарби і зволожувального розчину (1 – емульгована фарба, 2 – фарба без зволоження; розчин: 3 – на формі, 4 – відбитках).

На підставі результатів моделювання встановлено, що у зонах де щільність заповнення форми друкувальними елементами вища, більше фарби акумулюється на поверхні елементів фарбодрукарської системи, відповідно більша кількість зволожувального розчину емульгує у фарбу. Зі зростанням величини розщеплення фарби спостерігається зворотна тенденція.

Висновки. Запропонована інформаційна технологія може суттєво оптимізувати затрати на підготовку офсетних машин до друку.

Інформаційні джерела

1. Kipphan H. Handbook of Print Media: Technologies and Production Methods, 2014. – 1207 c. – (Springer Berlin Heidelberg).

УДК 004.4:355

ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ARCGIS PRO В СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Андрій ГАВРИСЬ
Вікторія ФІЛІППОВА
Кафедра цивільного захисту Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *In a paper examines the application of ArcGIS software in the field of civil protection to improve the effectiveness of emergency management and improve the decision-making process. The authors show the significant advantages of using ArcGIS Pro in the field of civil protection. The proposed recommendations can become the basis for improving the effectiveness of civil protection measures thanks to the introduction of modern GIS technologies.*

Keywords*: geographic information systems, risk monitoring, emergency management, hazard mapping, spatial analysis, crisis modeling, coordination.*

Анотація. *У роботі розглядається застосування програмного забезпечення ArcGIS Pro у сфері цивільного захисту для підвищення ефективності управління надзвичайними ситуаціями та покращення процесу прийняття рішень. Автори вказують на значні переваги використання ArcGIS Pro у сфері цивільного захисту. Запропоновані рекомендації можуть стати основою для підвищення ефективності заходів цивільного захисту завдяки впровадженню сучасних ГІС-технологій.*

Ключові слова: *геоінформаційні системи, моніторинг ризиків, управління надзвичайними ситуаціями, картографування небезпек, просторовий аналіз, моделювання кризових ситуацій, координація дій.*

Сучасний світ стикається зі зростаючою кількістю надзвичайних ситуацій природного, техногенного, соціального і воєнного характеру, які створюють серйозні загрози для життя людей, інфраструктури та екосистеми. В умовах урбанізації, зміни клімату та технічного прогресу забезпечення ефективного реагування на надзвичайні ситуації є однією з головних задач цивільного захисту. Для цього необхідні новітні технологічні рішення, які дозволяють оптимізувати процеси управління ризиками, моніторингу та ліквідації наслідків надзвичайних ситуацій.

Одним із таких рішень є використання геоінформаційних систем, які забезпечують просторовий аналіз та візуалізацію інформації. Програмне забезпечення ArcGIS Pro [1], розроблене компанією Esri, пропонує широкі

можливості для створення інтерактивних карт, аналізу даних у реальному часі та підтримки прийняття рішень.

Використовувати програмне забезпечення можна:

– на комп'ютері за допомогою ArcGIS Desktop, що вміщує в собі ArcMap для створення та редагування карт, аналізу просторових даних (геостатика, топографічний аналіз тощо) та інтеграції даних із різних джерел; і ArcGIS Pro для 3D-візуалізації та обробки великих обсягів даних, а також підтримки інтеграції з іншими програмами через Python та API;

– на мобільному телефоні через додатки ArcGIS Field Maps для збору геопросторових даних у реальному часі, навігації в полі з інтерактивними картами та внесення змін до даних безпосередньо під час роботи на місцевості; ArcGIS QuickCapture для швидкого збирання великого обсягу даних натисканням однієї кнопки, під час польових обстежень чи аварійних ситуацій та інтеграції з GPS для автоматичного збереження геолокації, чи Survey123, який розроблений з метою створення форм для опитувань та анкет із геологічною прив'язкою, задля збору структурованих даних та можливістю роботи в Offline з подальшою синхронізацією даних;

– на платформі ArcGIS Online для розробки інтерактивних карт і дашбордів, проведення геоаналітичних досліджень у хмарному середовищі з можливістю спільного доступу до карт та проєктів і роботи з великими наборами даних без потреби у високопродуктивному обладнанні.

Загалом програмне забезпечення ArcGIS Pro надає можливості для інтеграції та аналізу великих масивів даних із різних джерел, таких як супутникові знімки, демографічна статистика, дані про інфраструктуру та кліматичні показники, що дає змогу створювати детальні карти ризиків, які стають основою для стратегічного планування заходів із запобігання надзвичайним ситуаціям. *Наприклад*, за допомогою ArcGIS Pro можна ідентифікувати території, які найбільш уразливі до підтоплення [2], зсувів чи пожеж. Аналіз отриманих даних допомагає визначити пріоритетні напрямки роботи служб цивільного захисту, що в свою чергу підвищує ефективність їх діяльності.

Однією з функцій програмного забезпечення ArcGIS Pro є створення інтерактивних карт, які відображають актуальні дані про загрози [3]. Такі карти дозволяють не лише візуалізувати небезпеки, але й аналізувати їх динаміку виникнення в просторі та часі, як показано в роботі [4]. У надзвичайних ситуаціях, таких як землетруси чи техногенні аварії, ці карти стають важливим інструментом для координації дій рятувальних служб. За допомогою цього програмного продукту можна визначити маршрути евакуації, розміщення пунктів тимчасового перебування постраждалих або місця концентрації ресурсів. Інтерактивність цих карт забезпечують їхню високу ефективність у реальних умовах кризових ситуацій.

ArcGIS Pro дає змогу створювати моделі розвитку надзвичайних ситуацій, що є важливим для прогнозування наслідків та своєчасного реагування. Прикладом слугує моделювання поширення пожежі чи повені, що дає змогу оцінити території, які можуть постраждати, та спланувати дії з їх захисту. Моделювання також може бути використане для прогнозування зон впливу вибухів чи розливів небезпечних речовин, задля уникнення жертв серед населення та зменшення матеріальних втрат.

Раціональне використання ресурсів є ключовим завданням у надзвичайних ситуаціях, і ArcGIS Pro ефективно вирішує завдання такого типу, адже платформа надає можливість аналізувати дані про місцезнаходження техніки, персоналу та матеріальних запасів, визначаючи їхнє оптимальне розміщення. Тому, це програмне забезпечення можна використовувати для планування логістики, доставки гуманітарної допомоги чи розрахунку маршрутів евакуації з урахуванням стану дорожньої інфраструктури, що в свою чергу забезпечить економію часу та ресурсів, які є критично важливими в кризових умовах.

Застосування програмного забезпечення ArcGIS Pro у сфері цивільного захисту відкриває нові можливості для ефективного виявлення ризиків, картографування небезпек, моделювання сценаріїв надзвичайних ситуацій і оптимізації ресурсів. Його функціонал надає комплексний підхід до управління кризовими ситуаціями, сприяючи підвищенню ефективності роботи служб цивільного захисту.

Висновки. Впровадження програмного забезпечення ArcGIS Pro надає можливість більш ефективно реагувати на виклики сучасності, мінімізувати ризики для населення та інфраструктури, оптимізувати використання ресурсів, а також покращити координацію дій між різними структурами, залученими до ліквідації наслідків катастроф, що особливо важливо в умовах зростаючих загроз. Удосконалення методів використання ArcGIS Pro у сфері цивільного захисту є важливим напрямком для подальших досліджень, що сприятиме підвищенню рівня безпеки та захищеності суспільства.

Інформаційні джерела

1. Офіційний сайт ArcGIS Online. URL: https://esri.in.ua/.

2. Havrys A., Yakovchuk R., Pekarska O., Tur N. (2024). Use of the computer modelling for the analysis of dangerous areas during flooding of territories. Ecological Engineering & Environmental Technology, 25(4). URL: https://doi.org/10.12912/27197050/184265.

3. Grădinaru Anca & Dragomir P. I. & Badea Ana. (2022). Using gis tools to analyse emergency and civil protection situations specific issues.

4. Havrys A., Yakovchuk R., Pekarska O., Tur N. (2023). Visualization of Fire in Space and Time on the Basis of the Method of Spatial Location of Fire-Dangerous Areas. Ecological Engineering & Environmental Technology 24, pp. 28–37. URL: https://doi.org/10.12912/27197050/156971.

УДК 004.896

НАВЧАННЯ РОБОТІВ БАЛАНСУВАТИ: ДОСЯГНЕННЯ ТА ПРОБЛЕМИ

Денис КОТЕЛОВИЧ
Юрій БОРЗОВ
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *Balancing is a critical capability for legged robots, enabling stable locomotion and complex tasks in dynamic environments. The work deals with commercial projects, with a focus on their contribution to maintaining the balance of work, analyzes open projects and scientific developments, with their impact on the industry. The literature review includes control techniques based on physical models, reinforcement learning, simulation-to-reality, state estimation, and hardware innovations. It is necessary to identify key challenges and future directions in teaching robots to effectively maintain balance.*
Keywords: *robotics, robot, balance, reinforcement learning algorithms, simulation training.*

Анотація. *Здатність підтримувати рівновагу є критично важливою характеристикою для роботів з кінцівками, яка забезпечує стабільне пересування та виконання складних завдань у динамічних середовищах. В роботі розглянуто комерційні проекти, з фокусом на їхній вклад на підтримку рівноваги роботів, проаналізовано відкриті проекти та наукові розробки, з їхнім впливом на індустрію. Літературний огляд включає методи керування, що базуються на фізичних моделях, навчанням із підкріпленням, перенесення з симуляції в реальність, оцінку стану та інновації в апаратному забезпеченні. Необхідно визначити ключові виклики та майбутні напрями в навчанні роботів ефективно підтримувати рівновагу.*
Ключові слова: *робототехніка, робот, рівновага, алгоритми навчання з підкріпленням, імітаційне навчання.*

Ми живемо в епоху значних технологічних трансформацій, коли прориви в робототехніці, штучному інтелекті та обчислювальній техніці об’єднуються, щоб переосмислити наше бачення майбутнього. Швидкий прогрес у розробці людиноподібних і крокуючих роботів супроводжується досягненнями в інших областях, таких як великі мовні моделі, кордонні обчислення, передові сенсори, енергоефективні приводи та “біологічно натхненні” дизайни.

Ці інновації сприяють перетворенню роботів з громіздких прототипів у універсальні, людиноподібні машини. Досягнення у машинному навчанні, підкріплювальному навчанні та перенесенні з симуляції в реальність суттєво покращили здатність роботів адаптуватися і працювати в динамічних середовищах, тоді як апаратні розробки зробили їх легшими, маневренішими та енергоефективнішими.

У центрі цього трансформаційного процесу знаходиться проблема рівноваги, яка є фундаментальною здатністю для людиноподібних та багатоногих/крокуючих роботів. Рівновага важлива не лише для стабільного пересування з точки в точку, але й для виконання маніпуляційних та координованих рухів у динамічних і непередбачуваних середовищах, включаючи ті, що включають взаємодію з людьми.

Існує безліч провідних проектів та ініціатив у сфері роботів з ногами, які можна поділити на комерційні та науково-дослідні проекти.

Комерційні проєкти. Boston Dynamics; Tesla; Apptronik; Agility Robotics; Figure AI; UBTECH Robotics; Unitree Robotics; SoftBank Robotics; Kawada Industries і AIST та інші.

*Дослідницькі проєкти***.** Waseda University; NASA; RoMeLa (UCLA); Willow Garage; Noetix Robotics; Duke University; National Institute of Advanced Industrial Science and Technology (AIST) та інші.

Рисунок 1 – Комерційні проєкти

Балансування є ключовим для виконання складних завдань у крокуючих роботах: від забезпечення стабільного пересування до виконання маніпуляцій і координації рухів всього тіла. Для досягнення цього застосовуються різні підходи, що охоплюють як модельно-орієнтовані методи керування, так і алгоритми навчання з підкріпленням.

Традиційні підходи до балансування часто базуються на використанні математичних моделей динаміки робота. *Наприклад*, Лінійна модель інвертованого маятника (LIPM) стала основою для генерації стабільних шаблонів ходьби у двоногих роботів. Подальші розширення цієї моделі включають інтеграцію кінематики для забезпечення координації рухів всього тіла. Використання імпульсного контролю дозволило суттєво підвищити стабільність у роботах з торцевим керуванням, що робить їх більш надійними в багатозадачному середовищі.

Безпека та відповідність є критичними аспектами у взаємодії роботів із середовищем, особливо коли йдеться про взаємодію з людьми. Контроль імпедансу дозволяє роботам адаптувати жорсткість і гасіння коливань у су-

глобах, що дає змогу поглинати удари й підтримувати баланс під час зовнішніх впливів. Крім того, методи виявлення та реакції на зіткнення допомагають забезпечити як безпеку, так і збереження рівноваги.

Алгоритми навчання з підкріпленням (RL) набувають популярності як методи адаптивного керування балансом. *Наприклад*, алгоритми Proximal Policy Optimization (PPO) та Deep Q-Networks (DQN) використовуються для навчання роботів складній поведінці. Крім того, ієрархічні підходи до RL та імітаційне навчання дозволяють значно підвищити ефективність процесу, зокрема у складних сценаріях, таких як пересування по нерівних поверхнях.

Одним із викликів у балансуванні є розрив між симуляційним середовищем і реальними умовами. Техніки рандомізації середовища під час симуляцій дозволяють навчати роботів адаптивності, що підвищує їхню надійність у реальних умовах. Це особливо корисно для чотириногих роботів, які повинні зберігати рівновагу на різних типах поверхонь.

Точна оцінка стану робота є основою для управління балансом. *Наприклад*, поєднання кінематики ніг із даними інерційних сенсорів через фільтр Калмана (EKF) дозволяє покращити точність вимірювання. Використання сучасних систем сприйняття й планування дозволяє роботам ефективно орієнтуватися в динамічному середовищі, що є критичним для надійного балансування.

Ці методи демонструють значний потенціал у вдосконаленні здатності роботів до балансування, що є ключовим для їхнього успішного використання в складних і змінних середовищах.

Майбутні напрями

– Адаптивні стратегії управління: Гібридні методи, які поєднують моделі управління та навчання, можуть підвищити ефективність у динамічних умовах.

– Реальна реалізація: Розширення використання роботів у логістиці, охороні здоров’я та ліквідації наслідків стихійних лих залишається викликом.

– Інтеграція сенсорів: Впровадження високотехнологічних сенсорів для покращення точності балансування.

Висновки. В роботі розглянуто ключові досягнення у сфері балансування роботів, зосереджуючись на методах керування, підходах до навчання та інноваціях в апаратному забезпеченні. Незважаючи на значний прогрес, залишається низка викликів у покращенні адаптивності, ефективності та масштабованості роботів.

Подальші дослідження в цих напрямках сприятимуть створенню роботів, здатних ефективно функціонувати в динамічних та непередбачуваних середовищах.

Інформаційні джерела

1. Dario Amodei et al. Concrete Problems in AI Safety.
2. Marcin Andrychowicz et al. Hindsight Experience Replay.

3. Xue Bin Peng et al. “DeepMimic: example-guided deep reinforcement learning of physics-based character skills”.

4. Xue Bin Peng et al. “Sim-to-Real Transfer of Robotic Control with Dynamics Randomization”.

5. Andrei A. Rusu et al. Progressive Neural Networks.

6. John Schulman et al. Proximal Policy Optimization Algorithms.

7. John Schulman et al. Trust Region Policy Optimization.

8. Adrien Escande, Nicolas Mansard, and Pierre-Brice Wieber. “Hierarchical quadratic programming: Fast online humanoid-robot motion generation”.

9. Maurice Fallon et al. “An Architecture for Online Affordance-based Perception and Whole-body Planning”.

10. Chelsea Finn, Pieter Abbeel, and Sergey Levine. Model-Agnostic Meta-Learning for Fast Adaptation of Deep.

УДК 621.392

АЛГОРИТМІЗАЦІЯ РОЗРАХУНКУ ПАРАМЕТРІВ ЗАХИСНИХ ГІДРОТЕХНІЧНИХ СПОРУД

Максим МЕЛЬНИК
Юрій РУДИК
Львівський державний університет безпеки життєдіяльності м. Львів, Україна.

Abstract. *The purpose of carrying out various types of work is to gain knowledge about modern methods of calculating soil and other hydraulic structures using computer modeling, considering LIDAR systems, and mastering the general principles of modeling processes in embankments, excavations, and soils. Measures to ensure the stability of the hydraulic structure are justified through a comprehensive study of the stress-strain state of various rocks that make up the retaining dams, taking into account the forecast flooding of the rock massif and the seismicity of the territory.*

Keywords: *calculations, hydraulic structures, LIDAR, energy tension, martial law.*

Анотація. *Метою проведення робіт різного характеру є здобуття знань про сучасні методи розрахунку ґрунтових та інших гідротехнічних споруд за допомогою комп’ютерного моделювання, враховуючи системи ЛІДАР, оволодіння загальними принципами моделювання процесів у насипах, виїмках та ґрунтах. Заходи щодо забезпечення стійкості гідротехнічної споруди обґрунтовано завдяки комплексному дослідженню напружено-деформованого стану різноманітних порід, що складають огороджувальні дамби з урахуванням прогнозного обводнення породного масиву та сейсмічності території.*

Ключові слова: *розрахунки, гідротехнічні споруди, ЛІДАР, енергетична напруженість, воєнний стан.*

В умовах глобальної енергетичної напруженості та необхідності забезпечити енергетичний баланс України питання продовження ресурсу енергетичних підприємств є надзвичайно актуальним.

Макетні моделі – це реально існуючі моделі, що відтворюють модельовану систему в певному масштабі. Іноді такі моделі називаються масштабними. Параметри моделі і системи відрізняються між собою. Числове значення цієї відмінності називається масштабом моделювання, або коефіцієнтом схожості. Ці моделі розглядаються в рамках теорії подібності, яка в окремих випадках передбачає геометричну схожість оригіналу і моделі для відповідних масштабів параметрів. Прості макетні моделі – це пропорційно зменшені копії існуючих систем, які відтворюють основні властивості системи або об'єкта залежно від мети моделювання. Макетні моделі широко використовуються під час вивчення фізичних та аеродинамічних процесів, гідротехнічних споруд і багатьох інших технічних систем.

Аналіз основних положень методики оцінки надійності і безпеки гідротехнічних споруд в рамках системної теорії надійності [1–3] дозволяє констатувати, що ураховуючи конструктивні і компоновочні особливості гідротехнічних споруд та їх комплексів, можна стверджувати, що при оцінці надійності і безпеки гідротехнічної споруди за методом граничних станів розглядають один або декілька граничних станів. Можливість настання одного з граничних станів може бути пов'язана, або не пов'язана із настанням інших граничних станів. Тому, гідротехнічні споруди слід розглядати у якості системи, яка складається із певної кількості елементів, кожен з яких відповідає за опір досягненню граничного стану. Крім того, метод статистичних випробовувань може успішно використовуватись для оцінки надійності і безпеки гідротехнічних об'єктів в рамках системної теорії надійності при наявності між елементами системи кореляційних зв'язків [4]. Імовірнісний аналіз ризиків виникнення надзвичайного стану (або аварії) на гідротехнічних спорудах, гідровузлах чи каскадах гідровузлів є більш раціональним на відміну від детерміністичного підходу, заснованого на використанні норм і стандартів. Повний аналіз ризику виникнення надзвичайного стану надає більш повну уяву про надійність гідротехнічного об'єкта, оскільки розглядаються навантаження і впливи в усіх можливих діапазонах, а після оцінки виникнення надзвичайного стану можна дослідити внесок того чи іншого впливу або конструктивного рішення на загальну надійність об'єкта [5–7].

Раціональне та ефективне природокористування в сучасних умовах неможливе без оперативної об'єктивної інформації про стан земельного фонду країни. У свою чергу отримання достовірної та інформаційно насиченої інформації можливо лише з використанням дистанційних методів зондування поверхні Землі. Сьогодні для створення систем оперативної інформації про стан земельних ресурсів в Україні є всі умови, які базуються на існуючих системах наземних і аерокосмічних спостережень і методах дистанційного зондування (ДЗЗ).

Систематичне використання дистанційного зондування Землі дозволяє проводити кількісну і якісну оцінку стану ґрунтового покриву з необхідною періодичністю, одержувати інформацію з максимально можливою оперативністю, видавати своєчасні рекомендації по застосуванню регулюючих заходів. Аналіз наявного досвіду [8] використання космічних методів дослідження земельних ресурсів переконує в тому, що ці методи в найближчому майбутньому замінять традиційні способи одержання інформації про земельні ресурси, але ці методи не систематизовані. Широкий розвиток космічних методів вивчення земельних ресурсів і їхнє швидке впровадження у виробництво є нагальною потребою сьогоднішнього дня.

Вирішення цих задач має важливе значення для планування сільськогосподарських меліоративних заходів і для оцінки стану гідротехнічних споруд, дозволяє значно зменшити незаплановані витрати води. Найбільш перспективним є застосування дистанційних методів при визначенні вологості сільськогосподарських угідь для великих територій, зайнятих однорідними сільськогосподарськими культурами. Аерокосмічні методи використовуються також для складання нових і корегування існуючих ґрунтових та агрохімічних карт для потреб агросектора [8–10].

Отже, одним із стратегічних джерел інформації держави є використання інформаційних систем, і насамперед це пов’язано з впровадженням сучасних технологій на основі космічних систем дистанційного зондування поверхні землі. Сьогодні в космосі працюють десятки апаратів різних типів, що виконують збір даних різними дистанційними методами.

Встановлено, що перевагами дистанційних методів можна вважати оперативність; незалежність від погодних умов, добового чи сезонного періоду; можливість дослідження великих територій, включаючи важкодоступні місця; можливість проведення комплексного моніторингу, що охоплює різні характеристики досліджуваних об’єктів; відображення динаміки протікання процесів; картографування потенційно небезпечних ділянок. Встановлено, що для розвитку галузі дистанційного зондування, потрібно постійного удосконалювати технології ДДЗ та розширити ринок продукції ДДЗ.

Доведено, що спектрометричним методом дистанційного зондування можна успішно визначати ґрунтову вологість, кількість гумусу в ґрунті, розпізнавати і оцінювати рослинний покрив, оцінювати ступінь засміченості сільськогосподарських культур і їх ураженість різними шкідниками, визначати зараженість рослин важкими металами і нітратами, а так само ступінь забруднення ґрунтів нафтою і нафтопродуктами, розпізнавати і контролювати ерозійні процеси, контролювати деградації земель.

Висновки. Аналіз досвіду використання космічних методів дослідження земельних ресурсів переконує в тому, що ці методи в найближчому майбутньому в основному замінять традиційні способи одержання інформації про земельні ресурси. Розвиток космічних методів вивчення земельних ресурсів

і їхнє швидке впровадження у виробництво є нагальною потребою сьогоднішнього дня.

Подяка. Дана робота виконана завдяки грантовій підтримці Національного Фонду Досліджень України, реєстраційний номер проєкту 0123U103529 (2022.01/0009) "Оцінювання та прогнозування загроз відбудові та сталому функціонуванню об'єктів критичної інфраструктури" за конкурсом "Наука для відбудови України у воєнний та повоєнний періоди".

Інформаційні джерела

1. Величко С. В., & Дупляк О. В. (2024). Розрахунки гідротехнічних споруд з використання програмного комплексу GeoStudio: методичні вказівки до виконання лабораторних робіт.

2. Тимощук В. І., & Шерстюк Є. А. "Комплексна оцінка стану гідротехнічних споруд Ладижинської ТЕС у зв'язку з їх рекострукцією". (2022).

3. MURASOV, Rustam; TERTYSHNYY, Bohdan. Методика розрахунку наслідків при проривах (руйнування) гідротехнічних споруд критичної інфраструктури. Social Development and Security, 2022, 12.6. – С. 140–152.

4. Барбашин В. В., Мацько О. І., Убайдулаєв Ю. Н., & Толкунов І. О. Навчальний посібник. Локалізація та ліквідація надзвичайних ситуацій на гідротехнічних спорудах.

5. Алдашев С. А., Новіков О. М., Андрущак І. Є., Номіровський Д. А., Анікушин А. В., Пашко А. О., & Сіренко І. П. (2020). Журнал обчислювальної та прикладної. Order, (409).

6. Вайнберг А. І. Надійність та безпека гідротехнічних споруд : монографія. Харьків: Важпромавтоматика, 2008. 304 с.

7. Федоренко Ю. А. (2020, November). Моніторинг методів діагностики земної поверхні з допомогою дистанційного зондування землі для використання в аграрному секторі. In The 3 rd International scientific and practical conference–Priority directions of science and technology development (November 22–24, 2020) SPC–Sci-conf. com. ua‖, Kyiv, Ukraine. 2020. 1488 p. p. 509.

8. Байрак Г. Р. Аналіз рельєфу і природокористування рівнин заходу України за аерокосмічними даними: монографія. Львів: Видавничий центр ЛНУ ім. Івана Франка, 2007. 296 с.

9. Ковтун О. В. Фрагменти з історії використання дистанційних методів у картографуванні ґрунтів. Історичні записки: Збірник наукових праць. Східноукраїнський ун-т імені Володимира Даля. Луганськ, 2008. – С. 148–153.

10. Кравчук В. І., Сердюченко Н. М., Ковтуненко О. В. та ін. Основи методології моніторингу агроресурсів та прогнозування врожайності сільськогосподарських культур за проектом MARS./ Техніко-технологічні аспекти розвитку та випробування нової техніки і технологій для сільського господарства України: Зб. наук. праць. Дослідницьке: 2009. Вип. 13 (27). Кн. 2. – С. 3–14.

Напрям 13

ОРГАНІЗАЦІЯ БАЗ ДАНИХ І ЗНАНЬ

УДК 656.035.22, 004.65

ФОРМУВАННЯ ОБЛІКУ СХОВИЩА ДАНИХ ДЛЯ ОБЛІКУ ТРАНЗАКЦІЙ ПРОЇЗДІВ У МІСЬКОМУ ТРАНСПОРТІ

Володимир ЗАХАРЕНКО
Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут", м. Харків, Україна.

Abstract. *The use of databases for fare accounting in urban transport is a common and effective practice. In turn, the use of data warehouses in transport systems is of key importance for optimizing operations, analyzing performance and making data-based decisions.*

Keywords: *automated fare payment system, subject area, entity, data warehouse.*

Анотація. *Використання баз даних для обліку проїзду у міському транспорті є поширеною та ефективною практикою. Застосування, в свою чергу, сховищ даних у транспортних системах має ключове значення для оптимізації операцій, аналізу продуктивності та прийняття рішень на основі даних.*

Ключові слова: *автоматизована система оплати проїзду, предметна сфера, сутність, сховище даних.*

Використання баз даних для обліку проїзду у міському транспорті є поширеною та ефективною практикою. Бази даних дозволяють організувати зберігання, управління та обробку інформації про проїзди пасажирів, розклади, тарифи та інші пов'язані дані.

До основних способів використання баз даних для обліку проїзду в міському транспорті належать, *наприклад*, зберігання інформації про проїзди, коли база даних може містить інформацію про кожен проїзд пасажира, включаючи час, дату, місце посадки та висадки, номер маршруту та інші деталі. У свою чергу застосування сховищ даних (Data Warehouse) у базах даних транспортних систем має ключове значення для оптимізації операцій, аналізу продуктивності та прийняття рішень на основі даних.

Визначення предметної області проєктуємого сховища даних.

Предметна область сховища даних проїздів у громадському транспорті зосереджена на зберіганні інформації про проїзди та пов'язані з ними дані в системі громадського транспорту [1]. Це дозволяє відстежувати та керувати проїздами пасажирів, їх оплатою, маршрутами, розкладом та іншими

пов'язаними аспектами. Виходячи зі специфіки національного громадського транспорту у великих містах України, основними основними елементами, які можуть бути включені до такого сховища даних, є:

1. *Пасажири*: Інформація про пасажирів, включаючи унікальні ідентифікатори, контактні дані та можливу іншу персональну інформацію. Це допомагає відстежувати, скільки проїздів робить кожен пасажир.

2. *Проїзні квитки*: Дані про різні типи квитків та проїзних, їх ціни, терміни дії та умови використання.

3. *Тарифи*: Інформація щодо різних тарифних планів, включаючи одноразові поїздки, абонементи, знижки для певних категорій пасажирів тощо.

4. *Оплата проїзду*: Дані про оплату проїзду, включаючи способи оплати, транзакції, історію платежів та підтвердження оплати.

5. *Маршрути та розклад*: Інформація про різні маршрути громадського транспорту, точки зупинок, графік руху, терміни та інтервали руху маршрутами.

6. *Проїзний контроль*: Дані про контроль проїзду, перевірки квитків та інші механізми забезпечення оплати проїзду.

7. *Системи оплати*: Дані про системи оплати проїзду, такі як квиткові автомати, безконтактні картки, мобільні програми тощо.

8. *Аналітика та статистика*: Збір та аналіз даних для оцінки використання громадського транспорту, прогнозування пасажиропотоку та оптимізації маршрутів та розкладу.

Тобто проектоване СД повинна містити відомості про всі проведені транзакції: персональні дані громадян, які мають право на пільговий проїзд; дані про валідаторів – пристрої, які забезпечують списання коштів; інформацію про транспортні маршрути.

Визначення основних вимог до сховища даних.

На цьому етапі визначимо цілі та вимоги до нашого СД. Це включає виявлення сутностей, атрибутів, зв'язків між сутностями і вимог до продуктивності.

Виходячи з аналізу предметної області як сутності проектованого сховища даних виступатимуть:

– журнал активації/блокування карток пасажирів;
– електронний квиток;
– проїзна картка пасажира;
– індивідуальні дані пасажира;
– валідатор;
– журнал введення/зняття валідаторів;
– тип транспорту;
– маршрут;
– журнал введення/зняття маршрутів;
– журнал грошових операцій по карткам;
– журнал встановлення/зняття пільг пасажирам;

– інформація про пільги;
– журнал введення/призупинення пільг;
– додаткова інформація щодо пільг.

ER-диаграма взаємодії сутностей (зв'язку з-поміж них) проектованого сховища даних [2] представлена на рис. 1.

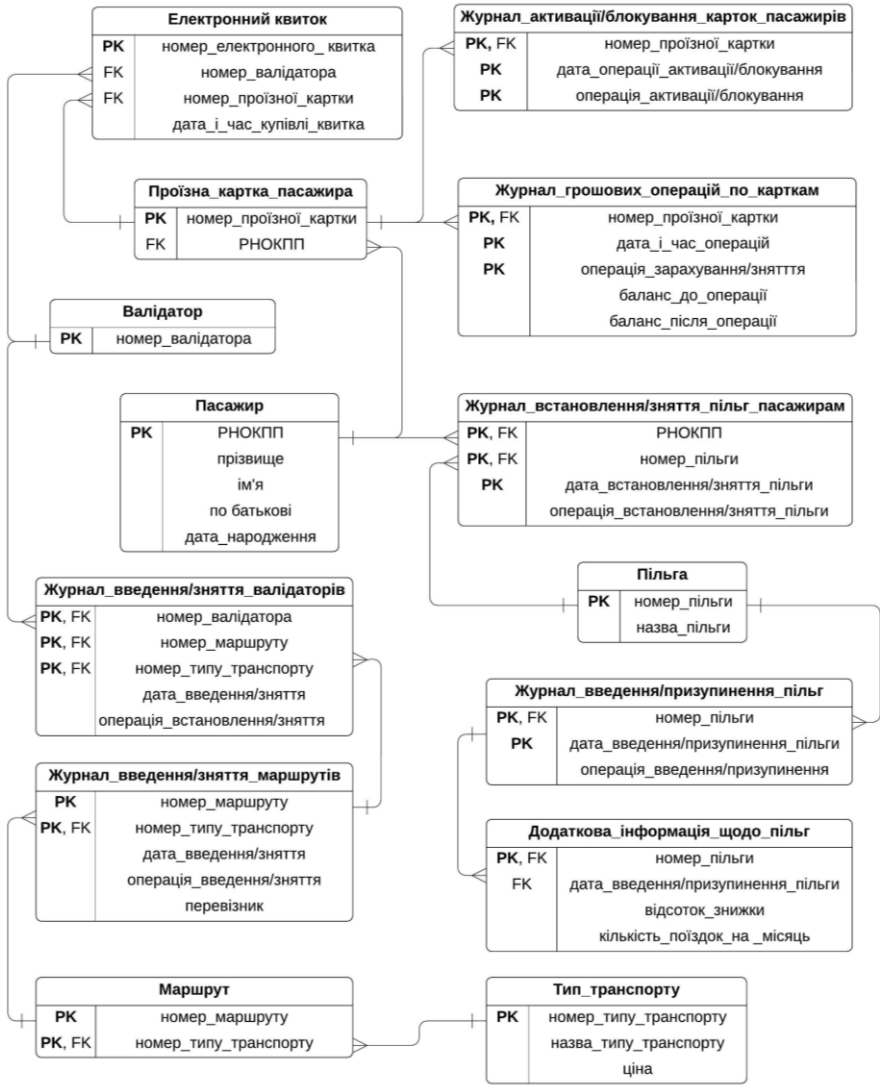


Рисунок 1 – Діаграма зв'язку та взаємодії основних сутностей сховища даних

Метою використання СД є створення таких видів звітів необхідні ефективного управління фінансовими і транспортними потоками у системі міського громадського транспорту:

1. Загальні звіти (кількісні).

– загальна кількість перевезених пасажирів у заданий час міським транспортом в цілому;

– загальна кількість перевезених пасажирів у заданий період різними перевізниками (трамвайними або тролейбусними депо, лініями метрополітену, власниками автобусного парку);

– загальна кількість перевезених пасажирів у заданий період часу за категоріями (мається на увазі пасажирів, які мають право на пільговий проїзд та пасажирів, які оплачують повну вартість проїзду);

– загальна кількість перевезених пасажирів у заданий час міським транспортом за обраними маршрутами.

2. Загальні звіти (фінансові).

– загальна сума грошових коштів за перевезення пасажирів у заданий період міським транспортом загалом відповідно до діючих тарифів;

– загальна сума грошових коштів за перевезення пасажирів у заданий період різними перевізниками (трамвайними або тролейбусними депо, лініями метрополітену, власниками автобусного парку);

– загальна сума коштів за перевезення пасажирів у заданий період часу за категоріями;

– загальна сума коштів за перевезення пасажирів у визначений період міським транспортом за обраними маршрутами.

3. Звіти щодо пільгових категорій громадян (персоніфіковані).

– персоніфіковані звіти щодо кількості проїздів за вибраний період часу за вибраними перевізниками;

– персоніфіковані звіти щодо загальної отриманої суми коштів за вибраний період часу за вибраними перевізниками.

Висновки. Результатом представленої дослідницької роботи є визначення та аналіз предметної області проектованого сховища даних поїздок у міському громадському транспорті, яка полягає в тому, що проектоване СД повинне містити відомості про всі проведені транзакції; пільгових категоріях громадян територіальної громади; персональні дані громадян, які мають право на пільговий проїзд; дані про валідаторів – пристрої, які забезпечують списання коштів; інформацію про транспортні маршрути міського транспорту. Іншим результатом проведених дослідження є визначення основних сутностей СД, їх атрибутів та схеми їх взаємодії.

Інформаційні джерела

1. Захаренко В. О. Модель побудови автоматизованої системи оплати проїзду та обліку пасажирів у міському громадському транспорті [Текст] / В. О. Захаренко // авіаційно-космічна техніка та технологія. – 2022. – No 4 (180). – С. 106–111. URL: https://doi.org/10.32620/aktt.2022.4.11.

2. Захаренко В. О., Туркін І. Б., Шевченко І. В. Проектування бази даних поїздок користувачів громадського транспорту з елементами технології Data Warehouse. Відкриті інформаційні та комп'ютерні інтегровані технології. – 2023. – No 97. – С. 205–216. URL: https://doi.org/10.32620/oikit.2023.97.13.

3. Morozov R. Prototype of Urban Transport Passenger Accounting System. Transportation Research Procedia Volume 68, 2023, pp. 468–474. URL: https://doi.org/10.1016/j.trpro.2023.02.063.

4. Nauman A. K., Nebel J. C., Khaddaj S. Scalable System for Smart Urban Transport Management. Journal of Advanced Transportation/ 2020 Article ID 8894705. URL: https://doi.org/10.1155/2020/8894705.

УДК 656.13:004.42

ІДЕНТИФІКАТОРИ СТРУКТУРНИХ І РЕЖИМНИХ ВЛАСТИВОСТЕЙ АВТОМОБІЛЬНИХ МАРШРУТІВ

Олександр ПРИДАТКО
Любомир ГАЩУК
Петро ГАЩУК
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.

Abstract. *When researching and organizing transport processes, it would be very convenient to operate databases on structural features of routes and on their speed potentials separately. This would significantly facilitate the accumulation and analysis of "transport data". The research found an algorithm that is convenient for practical use and artificially divides the characteristic parameters of the cargo movement route into structural and mode (high-speed) ones.*

Key words: *motor car, route, cargo speed, car performance, average values, road characteristic parameter, mode (speed) characteristic parameter.*

Анотація. *Досліджуючи й організовуючи транспортні процеси, було б дуже зручно оперувати базами даних про структурні особливості маршрутів і про їхні швидкісні потенції нарізно. Це істотно полегшило б нагромадження й аналіз "транспортних даних". В дослідженні віднайдено зручний для практичного використання алгоритм штучного поділу характеристичних параметрів маршруту пересування вантажів на структурні й режимні (швидкісні).*

Ключові слова*: автомобіль, маршрут, швидкість руху вантажу, продуктивність автомобіля, середні величини, шляховий характеристичний параметр, режимний (швидкісний) характеристичний параметр.*

Оцінювати маршрут так-чи-так доводиться за допомогою структурних і режимних параметрів [1, 2]. Структурні параметри визначають здебільшого те, як будова (структурна складність) маршруту позначатиметься на ефекти-

вності транспортного процесу, натомість режимні параметри мають характеризувати як інтенсивність пересування транспортних засобів окремими ділянками позначається на швидкості вантажного потоку і продуктивності автомобіля на маршруті загалом [3, 4].

Відобразімо для прикладу розвізний маршрут перевезень якнайзагальніше – пласким орієнтованим багатокутником-графом $0\to1\to2\ldots\to n\to0$ (рис. 1), вершинам якого відповідають автотранспортне підприємство (АТП, перевізник – точка 0) та пункти (осередки – точки $1, 2, \ldots, n$) продукування / споживання (завантаження / вивантаження) вантажів, а от сторонам цього багатокутника хай умовно відповідають ділянки шляху переміщення транспортного засобу та вантажів. Зокрема, ділянку маршруту 0–1 (до першого пункту завантаження) довжиною l_{01} та завершальну ділянку маршруту n–0 довжиною l_{n0} активний транспортний засіб долатиме марним (нульовим) ходом з деякими технічними швидкостями v_{01} та v_{n0} відповідно. Позначмо через l_{ik} – шлях між суміжними пунктами i та k продукування / споживання вантажу, який доводиться долати із середньою технічною швидкістю v_{ik}. Цілком подібно вигідно моделювати навіть так званий маятниковий цикл, рис. 2. Автомобіль здійснює n разів перевезення вантажу з пункту його продукування 1 у пункт його споживання 2 – кожного разу в кількості q. Прямий і зворотний шляхи однакові – завдовжки l, шляхи марного ходу з АТП на маршрут і з маршруту в АТП – відповідно l_0' і l_0''.

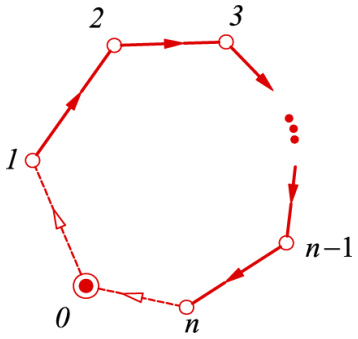


Рисунок 1 – Загальна схема-розгортка перевізного циклу

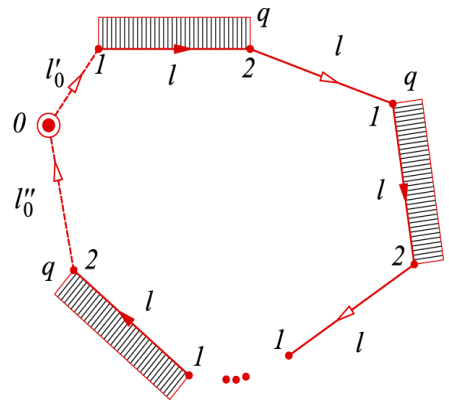


Рисунок 2 – Схема-розгортка маятникового циклу

Оцінюючи ефективність транспортного процесу, доводиться оперувати поняттям середньої технічної швидкости автомобіля, яку цього разу можна записати у вигляді:

$$v_{sr} = v_{\text{hm}r} = \frac{l_{12} + l_{23} + ... + l_{(n-2)(n-1)} + l_{(n-1)n}}{\frac{l_{12}}{v_{12}} + \frac{l_{23}}{v_{23}} + ... + \frac{l_{(n-2)(n-1)}}{v_{(n-2)(n-1)}} + \frac{l_{(n-1)n}}{v_{(n-1)n}}}. \qquad (1)$$

Величину (1) є формальні підстави називати гармонійним середнім зважених значень середніх локальних швидкостей v_{ik}, коли за ваги правлять відповідні шляхи l_{ik}. Натомість вираз:

$$v_{\text{am}r} = \frac{l_{12}v_{12} + l_{23}v_{23} + ... + l_{(n-2)(n-1)}v_{(n-2)(n-1)} + l_{(n-1)n}v_{(n-1)n}}{l} \qquad (2)$$

– це, зрозуміло, середнє арифметичне зважених шляхом величин v_{12}, v_{23}, …, $v_{(n-2)(n-1)}$, $v_{(n-1)n}$. Тут $l = l_{12} + l_{23} + ... + l_{(n-2)(n-1)} + l_{(n-1)n}$. Не менш важливим і корисним є й середнє геометричне тих самих зважених шляхом величин v_{12}, v_{23}, …, $v_{(n-2)(n-1)}$, $v_{(n-1)n}$

$$v_{\text{gm}r} = \frac{1}{l} \cdot \sqrt[n-1]{l_{12} \cdot l_{23} \cdot ... \cdot l_{(n-2)(n-1)} \cdot l_{(n-1)n}} \cdot \sqrt[n-1]{v_{12} \cdot v_{23} \cdot ... \cdot v_{(n-2)(n-1)} \cdot v_{(n-1)n}}. \qquad (3)$$

Фактична середня швидкість пересування автомобіля (1) завжди неменша за середню геометричну (3), яка своєю чергою завжди неменша за середню арифметичну (2). Отже середнє геометричне – завжди краща верхня оцінка фактичного середнього, ніж середнє арифметичне. Хай там як, а зазвичай у статистичному аналізі дуже часто перевагу все-таки надають оперуванню середніми арифметичними. І це здебільшого не створює особливих непорозумінь. Тож може справді нема сенсу перейматись вибором якогось справді об'єктивного середнього, що не зводиться до середнього арифметичного?

Очевидно, що вимірник середньої швидкости пересування автомобіля на маршруті цілком природно поєднує в собі у, так би мовити, консолідованому вигляді інформацію (дані) одночасно і стосовно структури маршруту, і стосовно швидкісних можливостей переміщення транспортного засобу окремими його ділянками. Але, впорядковуючи транспортні дані і формуючи транспортні процеси, було б дуже зручно оперувати даними про структурні особливості маршрутів і про їхні швидкісні потенції нарізно. І тут середнє арифметичне не може стати в пригоді.

Можна, зокрема, з'ясувати, що

$$v_{sr} \le \frac{l_{sr(a)}}{l_{sr(g)}} v_{sr(g)}, \qquad (4)$$

де

$$l_{sr(a)} = \frac{l_{12} + l_{23} + ... + l_{(n-2)(n-1)} + l_{(n-1)n}}{n-1} \qquad (5)$$

– арифметично середній шлях;

$$l_{sr(g)} = \sqrt[n-1]{l_{12} \cdot l_{23} \cdot ... \cdot l_{(n-2)(n-1)} \cdot l_{(n-1)n}} \qquad (6)$$

– геометрично середній шлях;

$$v_{sr(g)} = \sqrt[n-1]{v_{12} \cdot v_{23} \cdot ... \cdot v_{(n-2)(n-1)} \cdot v_{(n-1)n}} \qquad (7)$$

– геометрично середня швидкість. Зрозуміло, що $l_{sr(a)} / l_{sr(g)} \geq 1$, а тому співвідношення (17) можна ніби "підправити", записавши

$$v_{sr} \approx v_{sr(g)} = \sqrt[n-1]{v_{12} \cdot v_{23} \cdot ... \cdot v_{(n-2)(n-1)} \cdot v_{(n-1)n}} \; . \qquad (8)$$

Використання останньої формули (що є відображенням середнього геометричного) дає змогу уникнути зважування значеннями шляху осереднюваних значень швидкости. Очевидно також, що на противагу величині v_{sr} величина $\frac{l_{sr(a)}}{l_{sr(g)}} v_{sr(g)}$ в (4) побудована із застосуванням оператора усереднення до шляхових і швидкісних параметрів нарізно.

Величина $\frac{l_{sr(a)}}{l_{sr(g)}} v_{sr(g)}$, що фігурує у виразі (4), містить в своєму складі шляхові параметри $l_{sr(a)}$ і $l_{sr(g)}$ (див. (5), (6)), що характеризують структуру маршруту, та швидкісний параметр $v_{sr(g)}$ (див. (8)), що характеризує режим переміщення вантажу маршрутом. При цьому величина $l_{sr(a)}$ поєднує в собі інформацію про загальну довжину l маршруту та кількість ділянок $n-1$, на які він поділений. Поділ маршруту на ділянки однакової довжини можна було б назвати простим структуруванням – у цьому випадку $l_{sr(a)} = l_{sr(g)}$. А от чим більшим буде відношення $l_{sr(a)} / l_{sr(g)} > 1$, тим складнішою можна вважати структуру маршруту.

Через призму "регресії до середнього" здебільшого дивляться на все у світі. Беручи до уваги саме тенденційну регресію до середнього, величину v_{sr} хотілося б відповідно чи до (4), чи до (3) заступити чи величиною $v_{sr} \approx \frac{l_{sr(a)}}{l_{sr(g)}} v_{sr(g)}$, чи величиною $v_{sr} \approx \frac{l_{sr(g)}}{l} v_{sr(g)}$ Оцінка $v_{sr} \approx \frac{l_{sr(a)}}{l_{sr(g)}} v_{sr(g)}$ виглядає доволі привабливою змістом: за шляховий характеристичний параметр

править відношення $l_{sr(a)} / l_{sr(g)} \geq 1$, а за швидкісний – величина $v_{sr(g)}$ (середнє геометричне). Відповідно до неї формально $v_{sr} l_{sr(g)} \approx l_{sr(a)} v_{sr(g)}$ чи $\tau = l_{sr(a)} / v_{sr} \approx l_{sr(g)} / v_{sr(g)} = \tau'$. Найпростішою була б, звісно, оцінка $v_{sr} \approx v_{sr(g)}$: вона цілком ігнорує структуру маршруту, ніби натякаючи на те, що маршрути формують, керуючись певною логікою, що нівелює їхню особливість (раціональність несумісна з різноманітністю).

Висновки. Тож загалом вдалося з'ясувати:

1. Визначальним для оцінювання швидкости пересування вантажу маршрутом та визначення продуктивности автомобіля є середнє гармонійне значень швидкостей на окремих ділянках цього маршруту, зважених значеннями довжин цих ділянок. У разі, приміром, маятникового маршруту – це елементарне середнє гармонійне.

2. Із використанням класичних нерівностей можна знайти змістовні границі значень фактичної середньої гармонійної швидкости, які виражаються через елементарні класичні середні окремо шляхових і окремо швидкісних параметрів. Такі середні правлять за характеристичні параметри маршруту – шляхові й швидкісні.

3. В рамках обчислювальних операцій істинну середню гармонійну швидкість можна заступити середнім геометричним чи відповідною комбінацією елементарних середніх, покладаючись на ефект регресії даних до істинно середнього. Це істотно спрощує добування, перетворення й аналіз транспортних даних.

4. Критичне порівняння елементарних транспортних середніх (арифметичних, гармонічних, геометричних) дає підстави об'єктивно і всебічно оцінити особливості структурування маршрутів та особливості режимної організації перевезень вантажів.

Інформаційні джерела

1. Дмитриченко М. Ф., Яцківський Л. Ю., Ширяєва С. В., Докуніхін В. З. Основи теорії транспортних процесів і систем. Навчальний посібник для ВНЗ. – Київ: Видавничий Дім "Слово", 2009. 336 с. ISBN 978-966-8407-99-4.

2. Гащук Л., Гащук П. Теоретичні засади транспорту: Планування транспортних операцій: Навчальний посібник. – Харків: Видавництво "Діса плюс", 2024. – 256 с. ISBN 978-617-88122-93-5.

3. Ortúzar J. D., Willumsen L. G. Modeling Transport (4-th edition). – John Willey & Sons Ltd, 2011. – xx, 588 p. ISBN: 9781119993520.

4. Janić M. Transport Systems. Modelling, Planning, and Evaluation. – Taylor & Francis Group, LLC, 2017. – XVIII, 410 p. doi: 10.1201/9781315371023.

УДК 004.056.5:005.8

СИСТЕМА ТЕЛЕФОННОЇ КНИГИ ДЛЯ УНІВЕРСИТЕТУ

Маркіян МУСЯНОВИЧ
Діана РАЙТА
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *A phone book for the university has been proposed that provides multi-level access for teachers and students. The system allows faculty to view detailed information about their colleagues, including a photo, phone number, research papers, position, and email. Students have access to basic data, such as the name, title, and phone number of the teacher.*
Keywords*: phonebook, university, teacher, student, information access, access levels, scientific works, user profile.*

Анотація. *Запропоновано телефонну книгу для університету, яка забезпечує різнорівневий доступ для викладачів та студентів. Система дозволяє викладачам переглядати детальну інформацію про колег, включаючи фотографію, номер телефону, наукові роботи, посаду та електронну пошту. Студенти мають доступ до базових даних, таких як ім'я, посада та номер телефону викладача.*
Ключові слова*: телефонна книга, університет, викладач, студент, доступ до інформації, рівні доступу, наукові роботи, особистий кабінет.*

Для ефективної комунікації між студентами та викладачами в університеті важливо мати доступ до контактної інформації. Система телефонної книги для Львівського державного університету безпеки життєдіяльності надає таку можливість, забезпечуючи різні рівні доступу для викладачів та студентів. Реалізація цієї системи дозволить покращити внутрішню комунікацію, полегшуючи взаємодію між студентами та викладачами та сприяючи організації навчального процесу.

Система підтримує два типи користувачів – викладачів і студентів – кожен з яких має свої рівні доступу до інформації. Такий підхід дозволяє забезпечити конфіденційність і захист особистих даних, надаючи при цьому необхідний доступ до контактної інформації.

Викладачі мають можливість зареєструватися в системі з використанням логіну та паролю. Після авторизації вони можуть переглядати профілі колег, включаючи такі дані:

– фотографія – для ідентифікації особи;

– номер телефону – для безпосереднього зв'язку;

– наукові роботи – список опублікованих наукових статей та досліджень (якщо є);

– посада – поточна академічна посада викладача;

– електронна пошта – для офіційної комунікації.

Студенти також реєструються в системі з використанням логіну та паролю, проте мають обмежений доступ до інформації. Після входу в систему вони можуть переглядати лише базову інформацію про викладачів:

– ім'я та прізвище – для ідентифікації;

– посада – для розуміння академічного статусу викладача;

– номер телефону – для можливості зв'язку.

Система телефонної книги будується на основі архітектури MVC (рис. 1), яка дозволяє чітко розділити функціональні компоненти та полегшує підтримку й масштабування системи.

Містить опис користувачів (викладачів і студентів) та їх атрибутів, таких як ім'я, посада, номер телефону, електронна пошта, наукові роботи. Це забезпечує зв'язок з базою даних, де зберігається інформація про користувачів.

Рисунок 1 – Початковий набір базових MVC структур проєкту системи телефонної книги

Відповідає за обробку запитів користувачів, а також за їх скерування до відповідних методів сервісного рівня. *Наприклад*, "TeacherController" та "StudentController" реалізують логіку авторизації та забезпечують доступ до профілів викладачів згідно з правами доступу користувача.

Містить основну бізнес-логіку, яка дозволяє здійснювати пошук, фільтрацію та відображення профілів користувачів відповідно до рівня доступу. *Наприклад*, "UserService" обробляє логіку перевірки ролі користувача для визначення доступного обсягу інформації.

Висновки. Розробка системи телефонної книги для університету на основі архітектури MVC забезпечує зручний та безпечний доступ до інформації для студентів та викладачів. Завдяки різнорівневому доступу, система

дозволяє контролювати конфіденційність даних, одночасно надаючи користувачам необхідний обсяг інформації для ефективної комунікації.

Інформаційні джерела

1. Борзов Ю., Головатий Р., Магеровський Я. Особливості застосування комп'ютерного моделювання для покращення навчального процесу. Інформаційні технології розвитку змісту освіти. – 2019. – С. 80–81.

2. Хлевной О. В, Райта Д. А., Буряк Н. Є., Борзов Ю. О. визначення параметрів руху евакуаційних потоків із застосування штучних нейронних мереж. Вісник ЛДУ БЖД, 2023. №26. – С. 40–46.

3. Смотр О. О., Рашкевич М., Головатий Р., Мечус Х. Використання інструментарію інформаційних технологій для підвищення мотивації студента до навчання у форматі змішаної освіти. Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : Збірник наукових праць. Випуск 6. / За ред. М. С. Коваля, Н. Г. Ничкало. – Львів : ЛДУ БЖД, 2021. – С. 214–217.

УДК 004.65

ПРИНЦИП РОБОТИ БАЗ ДАНИХ ЗА МОДЕЛЛЮ КЛЮЧА ТА ЗАМКА

Олександр ПРИДАТКО
Любомир ГАЩУК
Петро ГАЩУК

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.

Abstract. *When working with databases, we often come across different ways of structuring data. But in general, regardless of the structure, access to data most often occurs in the form of matching the appropriate keys to the appropriate locks. The formation of databases, their structuring and searching for data in them are very similar to human thinking processes. So it is interesting how the analysis of databases can be optimized and developed, and how the analysis of human mental activity can help in this.*

Key words: *databases, artificial intelligence, keys and locks, tags, human mind.*

Анотація. *Працюючи з базами даних ми часто зустрічаємось з різними способами структуризації даних. Але в загальному, незалежно від структури, доступ до даних найчастіше відбувається у вигляді підбору відповідних ключів до відповідних замків. Формування баз даних, їх структуризація та пошук даних в них дуже схожі на процеси мислення людини. Тож цікавим є те, як можна оптимізувати та розвинути аналіз баз даних, та як в цьому може допомогти аналіз розумової діяльності людини.*

Ключові слова*: бази даних, штучний інтелект, ключі та замки, теги, людський розум.*

Більшість наукових моделей базується на певній інтерпретації людиною явищ які вона спостерігає або логічних висновків які вона робить в процесі осмислення. Як відомо, в способі роботи комп'ютерних систем лежить принцип процесу думки людини. Перші ЕОМ(електронно-обчислювальні системи) використовувались для швидкого проведення складних обрахунків (*наприклад*, для підбору варіантів коду для розшифрування таємних повідомлень під час другої світової війни). По суті їхньою задачею було спрощення роботи людини та її прискорення, збільшення ефективності та якості. Пізніше системи почали використовувати для обробки більш різноманітної кількості вхідних даних. У зв'язку з цим виникла потреба у організації даних, створення їх конкретної структури та оптимальних шляхів доступу до них. Так з'явилось поняття бази даних, як спеціальної конструкції де різні дані певним чином організовувались і з ними легко можна було вести роботу.

Часто ми стикаємось з неструктурованими даними, в яких немає прямого зв'язку. При цьому в нас виникає потреба структуризувати ці дані у відповідності до певних показників (критеріїв пошуку). Ці дані перетворюються в конкретну інформацію тоді, коли в них знаходиться зв'язок та ці дані інтерпретуються розумом людини. В основі формування бази даних стоїть розподіл розрізнених даних по певних критеріях. Таким чином зараз функціонує тегування, тобто пошук даних з допомогою ключових слів. Відповідно, чим більша кількість цих слів застосовується тим точнішим є пошук і вузькішим результат. Таким чином працює "запам'ятовування" та "згадування" інформації людиною.

Щоб запамятати велику кількість інформації, ми автоматично починає її організовувати в думках. Ми створюємо списки справ або ідей. Розділяємо їх на важливі та не важливі, на негайні та ті в яких є час на виконання. І відповідно таким чином нам легше працювати з такою інформацією. Той самий принцип використовується при структуризації даних в базах даних. Бази даних мають багато видів логічних конструкцій для розподілу даних. Так, це можуть бути "списки", "дерева рішень", "чорно-червоні дерева", тощо. Конструкції, як простіші так і складніші у відповідності до способу організації. І відповідно, для того щоб отримати доступ до шуканих, конкретних даних нам потрібні критерії пошуку, тобто "ключі", які відкривають "замки". Цікавим є те що в базах даних до одного "замка" може бути багато "ключів" і навпаки: один "ключ" може підійти до багатьох "замків". *Наприклад* при тегуванні ми можемо знайти одні і ті ж дані використовуючи різні ключові слова.

Пам'ять людини працює подібним чином. Якщо ми маємо багато речей, які потрібно тримати в пам'яті, ми підсвідомо починаємо всі ці речі класифікувати. Чим більше ми розділяємо речі в нашій пам'яті та чим більше у нас є класифікаторів, тим легше буде згадати потрібну інформацію та відділити її від всього іншого. Також варто сказати, що комірка з шуканими даними не є кінцевим результатом пошуку. Ця комірка може мати зв'язок з

низкою інших комірок з іншими даними які доповнюють пошук або просто є дотичними до них. Цих звязків може бути дуже багато і ці звязки між даними перетворюються у велику мережу. За рахунок структуризації даних та їх звязку з іншими даними і утворюється база даних.

Висновки. Як висновок ми можемо сказати що структури даних в інформаційних системах та запам'ятовування інформації в людській нервовій системі є дуже схожими. Тоді постає питання, що досконаліше і які межі розвитку є присутніми. Зрозуміло що електронні інформаційні системи можуть легко і швидко впоратися з великою кількістю даних, тоді коли людський розум на це не здатен. Електронні пристрої обробки інформації завжди покращуються і поступово отримують все більше потужності та можливостей, на що не здатен людський інтелект. Але людський розум здатен обробляти дані таким складним чином і робити настільки незвичайні висновки на що поки що не здатен комп'ютер. Хоч зараз штучний інтелект є на високому рівні і розвивається, він ще поки обробляє дані тільки тим чином який йому диктує людина. І саме людина інтерпретує отриманий результат і перетворює його на структуровану інформацію.

Тож можна сказати, що у плані структуризації баз даних а також пошуку в них конкретних даних є великий потенціал для розвитку. Також теперішній динамічний розвиток штучного інтелекту відкриває нові можливості для аналізу даних та їх інтерпретації. Що до ключів та замків: сучасна система тегування є дуже не досконалою тому з метою підбору потрібної або цікавої для користувача інформації різні структури постійно просять дозвіл на збір та обробку даних. Але в плані самого користувача ця система є не дуже ефективною. Алгоритми пошуку постійно модифікуються. Використовуючи нові можливості штучного інтелекту та поглиблюючи розуміння про розумові процеси людини, вже в найближчий час ми можемо чекати на еволюцію та перехід на новий рівень методів аналізу та обробки даних.

Інформаційні джерела

1. Survey of Text Mining I: Clustering, Classification, and Retrieval / Ed. by M. W. Berry. – 2004. – Springer, 2003. – 261 c.

2. Silberschatz Abraham, Sudarshan S. (2011). *Database system concepts* (вид. 6). New York: McGraw-Hill.

3. Structure, Models and Meaning: Is "unstructured" data merely unmodeled?, Intelligent Enterprise, March I, 2005.

4. Гороховатський В. О., Творошенко І. С. Методи інтелектуального аналізу та оброблення даних: навч. посібник. 2021.

5. Кучук Н. Г., Мерлак В. Ю., Скородєлов В. В. Метод зменшення часу доступу до слабкоструктурованих даних. Сучасні інформаційні системи = Advanced Information Systems. – 2020. – Т. 4, № 1. – С. 97–102.

Напрям 14

ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ ДАНИХ

УДК 004.272.25

ENHANCING VIDEO SEARCH WITH MULTI-MODAL LLM AND VECTOR EMBEDDING TECHNIQUES

Pavlo HIBEY
Volodymyr SABAT
Lviv Polytechnic National University, Lviv, Ukraine.

Анотація. *У цьому документі пропонується мультимодальний підхід до пошуку відео з використанням великих мовних моделей і векторних вставок для покращення розуміння та пошуку вмісту [1, 2].*

Ключові слова. *Пошук відео, великі мовні моделі, векторні вставки, мультимодальність.*

Abstract. *This paper proposes a multi-modal video search approach using large language models and vector embeddings to enhance content understanding and retrieval [1, 2].*

Keywords. *Video search, large language models, vector embeddings, multimodal.*

The ubiquity of video content on the internet has transformed the way we consume and interact with information. However, the abundance of video data has also created a pressing need for efficient and intelligent search capabilities that can effectively navigate and retrieve relevant video content [3].

Existing search engines primarily rely on text-based metadata, such as titles, descriptions, and tags, to index and retrieve video content [4]. While this approach can be effective for some queries, it fails to leverage the rich semantic information present in the visual and audio components of video data.

To address this limitation, researchers have explored the use of large language models and vector embeddings to enable more comprehensive and contextual video search.

Large language models have demonstrated remarkable capabilities in understanding and interpreting natural language, including the ability to comprehend and reason about multimodal information. By integrating these models into video search systems, researchers aim to enhance the understanding and interpretation of video content, enabling more accurate and relevant search results.

Additionally, vector embeddings offer a powerful way to represent and compare video content, allowing for more precise matching between user queries and video assets.

Methodology

This research paper proposes a multi-modal video search approach that leverages large language models and vector embeddings to improve the effectiveness and user experience of video search. The proposed system integrates language models to comprehend the semantic content of video data, including both textual metadata and the visual and audio components. Additionally, the system utilizes vector embeddings to represent and compare video content, enabling more precise matching between user queries and relevant video assets. This multi-modal approach aims to enhance the accuracy and relevance of video search results, providing users with a more intuitive and efficient way to navigate and discover video content on the internet. The key components of the proposed system include:

– integration of large language models to understand video semantics;
– utilization of vector embeddings to represent and compare video content;
– multimodal approach combining textual, visual, and audio information;
– improved accuracy and relevance of video search results;
– enhanced user experience for navigating and discovering video content.

Embedding video content

To effectively leverage the semantic information present in video data, the proposed system employs a multi-modal approach that integrates large language models and vector embeddings. Large language models, such as BERT [5] and GPT-4 [3], have demonstrated impressive capabilities in understanding and interpreting natural language, including the ability to comprehend and reason about multimodal information. By incorporating these language models into the video search system, the system can extract and understand the semantic content of video data, including both textual metadata and the visual and audio components of the video.

Additionally, the proposed system utilizes vector embeddings to represent and compare video content. Vector embeddings provide a powerful way to encode the rich semantic information present in video data, allowing for more precise matching between user queries and relevant video assets.

Challenges and Limitations

While the proposed system's integration of large language models and vector embeddings aims to enhance video search capabilities, there are potential limitations to this approach. Relying solely on language models and vector embeddings may overlook important contextual information and nuances that are difficult to capture through these techniques alone. Additionally, the performance of language models can be heavily dependent on the quality and breadth of the training data, which may

not always accurately reflect the diverse and evolving nature of video content on the internet. Furthermore, the use of vector embeddings, while providing a powerful way to represent video semantics, may introduce challenges in accurately measuring the complex and multifaceted relationships between video assets and user queries. A more holistic approach that combines various techniques, such as content-based and context-aware video analysis, may be necessary to achieve truly effective and comprehensive video search capabilities.

Information sources

1. Wang L., Yang N., Huang X., Yang L., Majumder R., & Wei F. (2023). Large Search Model: Redefining Search Stack in the Era of LLMs. ACM SIGIR Forum (Vol. 57, Issue 2, p. 1). Association for Computing Machinery. URL: https://doi.org/10.1145/ 3642979.3643006

2. Ning M., Zhu B., Xie Y., Lin B., Cui J., Yuan L., Chen D., & Li Y. (2023). Video-Bench: A Comprehensive Benchmark and Toolkit for Evaluating Video-based Large Language Models. arXiv (Cornell University). Cornell University. URL: https://doi.org/ 10.48550/ arxiv.2311.16103

3. Yang S., Walker J., Parker-Holder J., Du Y., Bruce J., Barreto A., Abbeel P., & Schuurmans D. (2024). Video as the New Language for Real-World Decision Making. arXiv (Cornell University). Cornell University. URL: https://doi.org/10.48550/arxiv. 2402.17139

4. Otto C., Springstein M., Anand A., & Ewerth R. (2019). Understanding, Categorizing and Predicting Semantic Image-Text Relations. URL: https://doi.org/10.1145/ 3323873.3325049

5. Thomason J., Venugopalan S., Guadarrama S., Saenko K., & Mooney R. J. (2014). Integrating Language and Vision to Generate Natural Language Descriptions of Videos in the Wild. International Conference on Computational Linguistics (p. 1218). http:// anthology.aclweb.org/C/C14/C14-1115.pdf

УДК 519.2:338.1

ПРОБЛЕМИ МОДЕЛЮВАННЯ ТА ВІЗУАЛІЗАЦІЇ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ПРОЦЕСІВ

Орест МИЩИШИН

Кафедра цифрової економіки та бізнес-аналітики. Львівського національного університету імені Івана Франка, м. Львів, Україна.

Abstract. *Research and modelling of socio-economic processes involves the transition from deterministic values to stochastic ones, which determines the use of normal distribution for economic parameters. The creation of time-varying stochastic models is possible on the basis of the theory of random processes.*

Key words: *socio-economic process, salary, stochastic model, normal distribution, size range of shoes.*

Анотація. *Дослідження та моделювання соціально-економічних процесів передбачає перехід від детермінованих величин до стохастичних, що визначає використання нормального розподілу для економічних параметрів. Створення змінних в часі стохастичних моделей можливе на базі теорії випадкових процесів.*

Ключові слова: *соціально-економічний процес, заробітна плата, стохастична модель, нормальний розподіл, розмірний ряд взуття.*

Вивчення економіку країни в цілому, окремих територій чи груп населення потребує аналізу її окремих метрик представлених у вигляді констант або змінних. Для опису агрегованих або усереднених значень використовують детерміновані величини. Узагальнені значення метрик не завжди дозволяють проаналізувати поведінку економічної системи чи дослідити процес впливу винагороди за виконану роботу на велику кількість працівників з різним рівнем заробітної плати. Отож для опису масових соціально-економічних явищ чи фінансових процесів використовують інший тип математичних понять – стохастичні величини. Стохастичні моделі для економіки вивчали і використовували, зокрема Бондаренко С. М. [1], Жлуктенко В. І., Бегун А. В. [2], Томашевський В. М., Жданова О. Г., Жолдаков О. О. [3].

Перший приклад побудови стохастичної моделі стосуються створення наближеної до реальності моделі величини заробітної плати, яка міняється в річному вимірі та стосується великої групи людей на великому підприємстві або територіальній одиниці.

Параметри стохастичної величини, яка описує заробітну плату в Україні в 2020–2022 роках мають наступні значення: математичне сподівання $m_{\_2020}$ = 10340 грн та середньоквадратичне відхилення $\sigma_{\_2020}$ = 1334 грн., $m_{\_2021}$ = 12993 грн та середньоквадратичне відхилення $\sigma_{\_2021}$ = 1429 грн., $m_{\_2022}$ = 14859 грн та середньоквадратичне відхилення $\sigma_{\_2022}$ = 1547 грн., $m_{\_2023}$ = 15778 грн та середньоквадратичне відхилення $\sigma_{\_2023}$ = 1676 грн. [4]. Для побудови моделі використано обернену функцію нормального розподілу NORMINV (Probability, mean, standard_dev) інструменту Excell, для аргументів mean = m, standard_dev = σ. Значення Probability задано випадковим чином за допомогою функції RAND(). Наступне завдання яке вирішено – групування усіх значень заробітної по групах з кроком групування 100 грн, для цього використано інструментарій Bing візуалізатора Tableau. Для агрегованого кількісного представлення розміри зарплатні згруповано з кроком 100 грн. та відображено у формі стовпцевої діаграми з візуалізацією заробітної плати кожного працівника (рис. 1).

Джерело: змодельовано автором на основі [4]

Також зрозуміло що заробітна працівників змінюється по-різному, тобто заробітні плати різних працівників не повинні повністю корелювати між собою. В моделі це забезпечується використання функції RAND() для моделювання заробітної плати окремо для різних років кожного окремо взятого працівника (рис. 1).

Рисунок 1 – Випадковий процес зміни стохастичних величин розподілу заробітної плати

При дослідженні соціально-економічних процесів стохастичний розподіл мають не тільки економічні та фінансові величини, але й антропометричні і навіть психологічні.

Проблема розподілу взуття та одягу за розмірами до цього часу досліджувалась мало [1]. На першому етапі дослідження було застосовано найпростіший підхід – закупити однакову кількість взуття різних розмірів. Наступний підхід дослідження включав експертну оцінку частоти розмірів жіночого взуття в Україні. На основі експертної оцінки за допомогою функції Гауса розраховано частотний набір жіночого розміру взуття для України. Параметри стохастичної величини, яка описує частотний набір становили середнє значення $m_{\_exp} = 38, \sigma_{\_exp} = 1{,}5$.

Також зібрано статистичні дані про антропометричні параметри 247 осіб жіночої статі. (рис 2). На основі статистичних даних за допомогою функції Гауса розраховано частотний набір розмірного ряду жіночого взуття для реальних людей в Україні. Параметри стохастичної величини, яка описує частотний набір розмірного ряду жіночого взуття, становили: середнє значення $m_{\_real} = 38{,}18$, середньоквадратичне відхилення $\sigma_{\_real} = 1{,}53$ (рис 2).

Джерело: сформовано автором на основі зібраних статистичних даних.

Ще одним етапом досліджень було порівняння зібраного антропометричного матеріалу для України з відповідними даними для США, а саме статистичного дослідження зробленого в Каліфорнійського університеті [5] про антропометричні параметри для більше ніж 500000 осіб жіночої статі.

Рисунок 2 – Частотний набір розмірного ряду жіночого взуття сформований на основі реальних даних та нормального розподілу для реальних даних

На основі статистичних даних за допомогою функції Гауса розраховано частотний набір жіночого розміру взуття для реальних мешканців в США. Параметри стохастичної величини, яка описує частотний набір для американських жінок становили: середнє значення m_usa =38, σ_usa =1,5.

Інформаційні джерела

1. Бондаренко С. М. Використання нормального розподілу Пуассона в системі управління якістю на підприємстві легкої промисловості. Економіка і суспільство. 2021. Випуск 32. URL: https://economyandsociety.in.ua/index.php/journal/article/view/840/807

2. Жлуктенко В. І., Бегун А. В. Стохастичні моделі в економіці.: Монографія. – К.: КНЕУ, 2005. – 352 с.

3. Томашевський В. М., Жданова О. Г., Жолдаков О. О. Вирішення практичних завдань методами комп'ютерного моделювання. – К.: Корнійчук, 2001. – 267 с.

4. URL: https://www.pfu.gov.ua/statystyka/pokazniki-serednoyi-zarobitnoyi-plat/arhiv-zapitannya-vidpovidi-peremishhenim-pokazniki-serednoyi-zarobitnoyi-plat/

5. URL: https://ukrayinska.libretexts.org/Математика/Прикладна_математика/ Бізнес_обчислення_з_Excel_(May_i_Bart)/07%3A_Інтеграція/7.06%3A_Нормальний_розподіл_-_Розширений_числовий_приклад

УДК 629.735.05:621.391

ДОСЛІДЖЕННЯ ВПЛИВУ ЗОВНІШНІХ ФАКТОРІВ НА ЯКІСТЬ ЗВ'ЯЗКУ З БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ В УМОВАХ ОПЕРАТИВНИХ ДІЙ

Денис ЖУКОВ
Іван РОВЕЦЬКИЙ

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The study investigates the impact of external factors on the quality of communication with unmanned aerial vehicles (UAVs) during operational activities. Key signal parameters affected by interferences are analyzed. Recommendations for improving communication stability are provided.*

Keywords: *unmanned aerial vehicles, communication quality, operational activities, external factors, radio communication.*

Анотація. *У роботі досліджено вплив зовнішніх факторів на якість зв'язку з безпілотними літальними апаратами (БПЛА) в умовах оперативних дій. Проаналізовано ключові параметри сигналу, які змінюються під дією перешкод. Наведено рекомендації щодо покращення стабільності зв'язку.*

Ключові слова: *безпілотні літальні апарати, якість зв'язку, оперативні дії, зовнішні фактори, радіозв'язок.*

Сучасні безпілотні літальні апарати (БПЛА) відіграють важливу роль у різних сферах – від військових операцій до рятувальних місій та моніторингу навколишнього середовища. Їх ефективне використання залежить від стабільності та якості зв'язку, який забезпечує передачу даних і команд в реальному часі. Однак зовнішні фактори, такі як погодні умови, електромагнітні перешкоди та географічні особливості, можуть значно впливати на цей зв'язок.

Дослідження впливу таких факторів є важливим для покращення стабільності роботи БПЛА, особливо в умовах оперативних дій, де від швидкості й точності передачі інформації часто залежить результат виконання завдань.

Мета роботи: метою роботи є визначення основних зовнішніх факторів, які впливають на якість зв'язку з безпілотними літальними апаратами, та розробка рекомендацій для забезпечення стабільності зв'язку в умовах оперативних дій.

Методологія дослідження: для досягнення поставленої мети проведено аналіз літературних джерел, а також експериментальні дослідження із використанням симуляційного моделювання умов зв'язку. Моделювання враховувало вплив погодних умов (дощ, туман, вітер), електромагнітних перешкод і особливостей рельєфу місцевості. Проведено аналіз змін основних параметрів сигналу, таких як потужність, затримка та коефіцієнт помилок.

Основні результати: у результаті дослідження встановлено, що найбільший вплив на якість зв'язку з безпілотними літальними апаратами мають погодні умови, такі як сильний дощ та туман. Зокрема, ці фактори спричиняють значне затухання сигналу, що знижує його потужність на 20–30% у порівнянні з нормальними умовами. Електромагнітні перешкоди, зокрема від роботи інших радіоелектронних пристроїв, збільшують коефіцієнт помилок у передачі даних, що може ускладнювати виконання критичних завдань.

Дослідження також показало, що рельєф місцевості впливає на затримку сигналу та стабільність зв'язку. Найгірші показники фіксувалися в умовах гірської місцевості, де через перешкоди сигналу коефіцієнт помилок зростав удвічі.

Рекомендації для покращення зв'язку включають використання антен з підвищеною потужністю та адаптивні алгоритми корекції сигналу, які можуть зменшити вплив зовнішніх факторів. Графічне зображення процесу збору інформації під час польоту та прийняття рішень в залежності від ситуацій подане на рисунку 1.

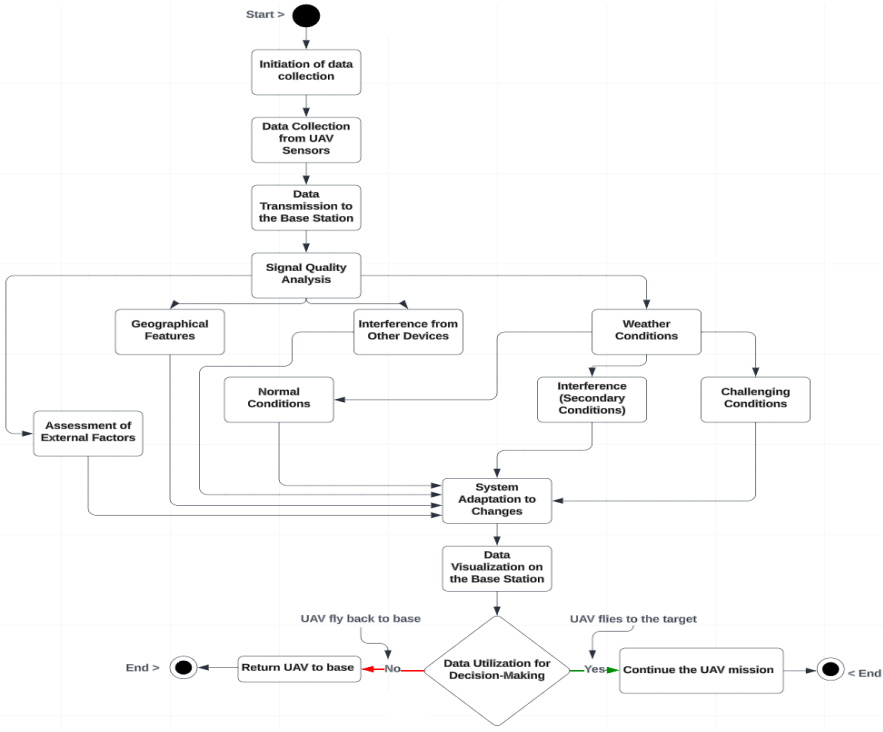


Рисунок 1 – Процес збору інформації під час польоту та прийняття рішень в залежності від ситуацій [5]

З даної блок-схеми можна зробити висновок, що процес збору інформації під час польоту та прийняття рішень в залежності від ситуацій являє собою високонавантажену розподілену паралельну систему.

Висновки. Дослідження показало, що зовнішні фактори, такі як погодні умови, електромагнітні перешкоди та рельєф місцевості, значно впливають на якість зв'язку з безпілотними літальними апаратами. Найбільш критичним є затухання сигналу під час несприятливих погодних умов і підвищення коефіцієнта помилок через електромагнітні перешкоди.

Впровадження технічних заходів, зокрема використання потужніших антен і алгоритмів адаптивної корекції сигналу, може суттєво зменшити вплив негативних факторів та забезпечити стабільність зв'язку. Подальші дослідження можуть бути спрямовані на розробку інноваційних систем зв'язку, здатних працювати в умовах значних перешкод.

Інформаційні джерела

1. Anderson J. D. Communication Systems for Unmanned Aerial Vehicles. IEEE Press.
2. Гончаренко І. М. Особливості функціонування БПЛА в умовах впливу радіоперешкод.
3. Li X., & Wang Y. Impact of Weather Conditions on UAV Signal Stability. Journal of Aeronautical Engineering.
4. Ткаченко О. В., Смірнов П. І. Аналіз ефективності систем зв'язку в складних умовах місцевості // Вісник авіаційних технологій.
5. Zhang T., & Lin H. Advances in Adaptive Signal Processing for UAV Communication. Wireless Networks.

УДК 004.89

РОЗПІЗНАВАННЯ ЗГЕНЕРОВАНИХ ШТУЧНИМ ІНТЕЛЕКТОМ ЗОБРАЖЕНЬ АБО ВІДЕО МАТЕРІАЛІВ

Станіслав ЛАТИШЕВ
Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The recognition of generated images and videos is a crucial area of research, particularly for countering disinformation and enhancing security. This article explores key methods for detecting AI-generated content, including metadata analysis, visual anomalies, and chromatic and textural signals. Special attention is given to deepfakes, a technology that enables hyper-realistic manipulations using deep neural networks. Issues of detail accuracy, motion synchronization, and audio discrepancies in such materials are highlighted. The importance of improving detection algorithms and fostering critical thinking is emphasized as essential measures for preserving informational integrity in the digital transformation era.*

Keywords: *artificial intelligence, generated images, deepfakes, content recognition, neural networks, media literacy, information security.*

Анотація. *Розпізнавання зображень і відеоматеріалів, згенерованих штучним інтелектом, є важливим напрямом сучасних досліджень, зокрема в контексті протидії дезінформації та забезпечення безпеки. У статті розглянуто ключові методи розпізнавання контенту, такі як аналіз метаданих, візуальних аномалій, хроматичних та текстурних сигналів. Особливу увагу приділено глибоким фейкам – технології, яка дозволяє створювати надреалістичні підробки з використанням глибоких нейронних мереж. Розкрито проблеми точності передачі деталей, рухів та звуків у таких матеріалах. Підкреслюється важливість вдосконалення алгоритмів розпізнавання та розвитку критичного мислення для захисту інформаційної цілісності в епоху цифрових трансформацій.*

Ключові слова: *штучний інтелект, згенеровані зображення, глибокі фейки, розпізнавання контенту, нейронні мережі, медіаграмотність, інформаційна безпека.*

Вступ. Штучний інтелект (ШІ) стрімко розвивається, генеруючи високоякісний візуальний та відеоконтент. Це відкриває нові можливості для створення контенту, але водночас породжує виклики, пов'язані з ідентифікацією його автентичності. Розпізнавання ШІ-згенерованих зображень і відео має важливе значення в контексті протидії дезінформації, захисту прав людини та забезпечення інформаційної безпеки. Дослідження в цій сфері зосереджені на виявленні особливостей, характерних для створеного ШІ контенту, зокрема за допомогою алгоритмів глибокого навчання, генеративних змагальних мереж (GAN) та інших передових технологій.

Аналіз останніх публікацій та матеріалів показує, що основні аспекти розпізнавання ШІ-згенерованого контенту наступні:

– використання нейронних мереж;
– візуальні аномалії;
– аналіз метаданих;
– хроматичні та текстурні сигнали.

Глибокі нейронні мережі, такі як згорткові (CNN) та рекурентні (RNN), відіграють ключову роль у розпізнаванні згенерованого контенту [1]. CNN здатні аналізувати зображення для виявлення аномалій, характерних для ШІ, тоді як RNN використовуються для обробки відео шляхом аналізу послідовності кадрів. Ефективність таких методів значною мірою залежить від якості навчання моделей і доступу до великих та репрезентативних наборів даних.

Одним із ключових індикаторів ШІ-згенерованих зображень є візуальні аномалії, які проявляються у неприродній геометрії об'єктів, некоректному відображенні світла і тіней або повторюваних візерунках [2]. *Наприклад*, текстури в таких зображеннях можуть бути надмірно гладкими або деталізованими, позбавленими природної нерівномірності. Крім того, "моторошна долина" є характерною для людських облич, створених ШІ: незначні спотворення рис чи неприродні вирази можуть викликати відчуття дискомфорту у глядачів.

Метадані, які супроводжують цифрові зображення, часто можуть слугувати індикатором їх походження. Зображення, створені ШІ, зазвичай мають обмежену кількість метаданих або невідповідності, що свідчать про штучне

походження контенту. *Наприклад*, відсутність інформації про модель камери чи геолокацію може бути ознакою згенерованого зображення.

Штучний інтелект має тенденцію до перебільшення або применшення кольорової насиченості [3]. Це може проявлятися у формі надто яскравих або неприродно приглушених зображень. Аналогічно, текстури в ШІ-згенерованих зображеннях часто не відповідають реалістичним фізичним властивостям.

Окремо можливо виділити глибокі фейки (deepfakes), які представляють особливий виклик. Ця технологія використовує глибокі нейронні мережі для накладання існуючих відео чи зображень на вихідний матеріал, створюючи надреалістичні підробки. Їх використання варіюється від розважальних цілей до поширення дезінформації. Основні проблеми в розпізнаванні глибоких фейків включають [3]:

Невідповідність рис обличчя та експресії. Глибокі фейки можуть демонструвати аномалії, такі як неприродне моргання, невідповідність виразів обличчя чи асинхронність між рухом губ і промовою.

Аномалії руху та синхронізації. Штучно створені відео часто мають неприродні рухи або розбіжності між руками губ і звуками.

Слухові розбіжності. Глибокі фейки можуть мати неприродне звучання голосу, що відрізняється від оригінального мовного патерну.

Висновки. Розпізнавання ШІ-згенерованого контенту є багатогранним завданням, що поєднує технічні аспекти з соціальними викликами. Одним із ключових питань є пошук балансу між автоматизацією процесу розпізнавання та розвитком критичного мислення у користувачів. По мірі вдосконалення алгоритмів ШІ технології розпізнавання також потребують постійного розвитку. Використання комбінації методів, таких як аналіз метаданих, виявлення візуальних аномалій і розпізнавання глибоких фейків, сприятиме підвищенню точності та надійності. Розвиток технологій штучного інтелекту та зростання поширеності згенерованого контенту підкреслюють важливість розпізнавання таких матеріалів. Використання сучасних алгоритмів, включаючи нейронні мережі, аналіз метаданих та інші методи, є важливим інструментом для забезпечення інформаційної безпеки. Водночас важливо розвивати медіаграмотність і культуру критичного споживання контенту, щоб протистояти потенційним загрозам.

Інформаційні джерела

1. Як розпізнати зображення, створені штучним інтелектом, або підроблені відео. URL: https://skimai.com/uk/як-розпізнати-зображення-створені-шт/#4_Ways_to_Spot_an_AI-Generated_Image (дата звернення: 18.11.2024).

2. Як розпізнавати зображення, згенеровані AI? URL: https://medium.com/@iryska_burdiug/як-розпізнавати-зображення-згенеровані-ai-28bdefa064f0 (дата звернення: 18.11.2024).

3. Як розпізнавати зображення, згенеровані AI. Komarov.Design – Блог #1 про графічний UI/UX дизайн в Україні. URL: https://www.komarov.design/iak-rozpiznavati-zobrazhiennia-zghienierovani-ai/ (дата звернення: 18.11.2024).

УДК 004.032.26

АНАЛІЗ МЕТОДІВ КОМП'ЮТЕРНОГО ЗОРУ ДЛЯ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ

Мар'ян ДАВИДКІН
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *An overview of the main computer vision (CV) methods used for processing and analyzing visual information is given, including image classification, object identification, object tracking, semantic segmentation, and instance segmentation. The importance of deep learning methods for solving complex computer vision problems is considered the use of the Mask R-CNN architecture for instance segmentation.*
Keywords: *computer vision, neural networks, machine learning, image processing, object recognition.*

Анотація. *Здійснено огляд основних методів комп'ютерного зору (CV), що використовуються для обробки та аналізу візуальної інформації, серед яких: класифікація зображень, ідентифікація об'єктів, відстеження об'єктів, семантична сегментація та сегментація екземплярів. Розглянуто важливість методів глибокого навчання для розв'язання складних завдань комп'ютерного зору, зокрема використання архітектури Mask R-CNN для сегментації екземплярів.*
Ключові слова: *комп'ютерний зір, нейромережі, машинне навчання, обробка зображень, розпізнавання об'єктів.*

Машинне навчання (ML) є однією з найбільш швидкозростаючих технічних галузей [1–3]. Технологія ML відіграє ключову роль у багатьох аспектах сучасного суспільства, зокрема у веб-пошуку, фільтрації інформації, системах рекомендацій на різних платформах. Сучасні досягнення в методах машинного навчання відкривають нові можливості для наукових досліджень, забезпечуючи доступ до ефективних інструментів [4]. Комп'ютерний зір (CV) – це галузь штучного інтелекту, яка дозволяє комп'ютерним системам аналізувати та інтерпретувати візуальну інформацію. Сучасні системи комп'ютерного зору можуть використовувати дані, як з камер чи різних датчиків у режимі реального часу, так і обробляти готові набори даних. Використовуючи передові методи для обробки та аналізу зображень і відео, технологія CV дає можливість комп'ютерам розпізнавати об'єкти та відповідно реагувати на них.

Перші експерименти із комп'ютерним зором розпочались у 1959 році, коли нейрофізіологи показували кішці серію зображень, намагаючись вивчити реакцію її мозку [5]. З'ясувалося, що перша реакція виникає на контрастні краї та лінії, що свідчить про те, що обробка зображень розпочинається з найпростіших елементів. У цей же час була створена перша технологія комп'ютерного сканування зображень, що дозволила комп'ютерам оци-

фровувати та аналізувати зображення. Технологія оптичного розпізнавання символів (OCR) було вперше презентовано у 1974 році, яка забезпечувала розпізнавання тексту, надрукованого будь-яким шрифтом чи гарнітурою. Удосконалена версія цієї технології для розпізнавання символів (ICR) дозволяє за допомогою нейронних мереж розшифровувати рукописний текст. У 1982 році нейробіолог Девід Марр дослідив, що зір працює за ієрархічним принципом, і розробив алгоритм, який забезпечував виявлення країв, кутів, кривих та інших базових форм. У 2010 році став доступним набір даних ImageNet, який містив мільйони зображень, розподілених за тисячами категорій об'єктів, що стало основою для CNN та моделей глибокого навчання, які використовуються сьогодні.

До технік комп'ютерного зору відносяться: класифікація зображень, ідентифікація об'єктів, відстеження об'єктів, семантична сегментація та сегментація екземплярів.

Класифікація зображень є процесом розподілу візуальних об'єктів до попередньо визначених класів. Цей процес здійснюється за допомогою алгоритмів, що аналізують візуальний вміст зображення та класифікують його на основі шаблонів. Процес класифікації включає етапи: збору даних, формування набору для навчання моделі, що складається з N зображень, кожне з яких асоційоване з одним із K класів, та визначення належності зображення до певного класу. Існують різні типи класифікацій зображень, серед яких: бінарна, що передбачає розподіл зображень на два взаємовиключні класи; багатокласова, у якій зображення відносяться до одного з кількох взаємовиключних класів, при цьому кожне зображення належить тільки до одного класу; багатоміткова, де зображення може бути віднесене до кількох класів одночасно; ієрархічна, що передбачає поділ зображень за ієрархічною структурою класів.

Ідентифікація об'єктів є методом комп'ютерного зору, що полягає у визначені та локалізації об'єктів на цифрових зображеннях. Процес ідентифікації включає класифікацію та локалізацію об'єктів. Локалізація об'єкта визначає його розташування на зображенні за допомогою обмежувальної рамки, в той час як класифікація об'єктів дозволяє віднести кожен виявлений об'єкт до відповідної категорії. Метод виявлення об'єктів об'єднує ці задачі, що дозволяє одночасно оцінювати як місцезнаходження, так і тип об'єктів на одному або декількох зображеннях. Процес виявлення об'єктів охоплює кілька етапів: попередній аналіз зображення, вибір архітектури моделі ідентифікації та визначення розміру об'єкта. Модель виявлення об'єктів виконує ідентифікацію та класифікацію областей, враховуючи такі візуальні характеристики, як форма, колір і розмір, використовуючи попередньо визначені набори даних.

Відстеження об'єктів є процесом визначення місцезнаходження об'єкта або декількох об'єктів на відео в реальному часі. Відстеження забезпечує ідентифікацію та позиціонування об'єкта під час його руху в межах деякої кількості кадрів, враховуючи зміни в його формі, розмірах, орієнтації. Ме-

тоди відстеження об'єктів можна поділити на два типи залежно від моделі спостереження: генеративні та дискримінаційні. Генеративні методи використовують моделі для опису видимих характеристик об'єкта та мінімізують помилку реконструкції при його пошуку, подібно до методу PCA. Дискримінаційні методи застосовуються для відокремлення об'єкта від фону і є більш надійними. Для таких задач зазвичай використовують дві основні моделі нейронних мереж: автоенкодер з обмеженою активацією (SAE) та згорткові нейронні мережі (CNN).

Семантична сегментація є технікою, що визначає, де на піксельному рівні закінчується один об'єкт, і починається інший. Цей процес складається з двох етапів: на першому визначаються семантичні цільові класи, на другому кожен піксель зображення відноситься до одного з цих класів. Крім класифікації, де система комп'ютерного зору визначає класи об'єктів, вона також повинна виявляти їхні межі. Процес сегментації є важливим для комп'ютерного зору, оскільки він поділяє зображення на групи пікселів, які потім можна класифікувати.

Сегментація екземплярів – це техніка, у якій класифікуються не лише пікселі зображення, але й виділяються окремі об'єкти одного класу, призначаючи кожному з них унікальну мітку. Сегментація екземплярів вимагає значно складніших підходів у порівнянні із семантичною сегментацією. Техніка застосовується до зображень, які містять кілька об'єктів, що перекриваються, і де потрібно не тільки класифікувати ці об'єкти, а й визначати їхні межі та взаємозв'язки. Один з основних підходів для вирішення задачі сегментації екземплярів полягає в застосуванні моделей на основі нейронних мереж, зокрема архітектури Mask R-CNN.

Висновки. Таким чином розглянуті техніки комп'ютерного зору, такі як класифікація зображень, ідентифікація об'єктів, відстеження об'єктів, семантична сегментація та сегментація екземплярів, займають важливе місце в сучасних системах обробки зображень.

Інформаційні джерела

1. Jordan M., Mitchell T. Machine learning: Trends, perspectives, and prospects. Science. – 2015. – С. 255–260.

2. Domingos P. A few useful things to Know about machine Learning. Communications of the acm. – 2012. – №55. – С. 78–87.

3. Riley P. Three pitfalls to avoid in machine learning. Nature. – 2019. – №572. – С. 27–29.

4. Mjolsness E., De Coste D. Machine Learning for Science: State of the Art and Future Prospects. Science. – 2001. – №293. – pp. 2051–2055.

5. Demush R. A Brief History of Computer Vision (and Convolutional Neural Networks). Hackernoon. – 2019. URL: hackernoon.com/a-brief-history-of-computer-vision-and-convolutional-neural-networks-8fe8aacc79f3.

УДК 004.928

АНАЛІЗ МЕТОДІВ ІНТЕРПОЛЯЦІЇ ЗНАЧЕНЬ КЛЮЧОВИХ КАДРІВ У КОМП'ЮТЕРНІЙ АНІМАЦІЇ

Ростислав КАЧУР
Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *An overview of the concepts and principles used in computer animation is provided. The components that must be considered when performing animation tasks are considered, including the differences between interpolation and approximation of curves, the complexity of interpolation equations and the concept of curve smoothness. The main methods of interpolation of values are analyzed, including linear, trigonometric, cubic and spherical.*

Keywords: *computer graphics, animation, value interpolation, 3D visualization.*

Анотація. *Проведено огляд понять і принципів, що застосовуються в комп'ютерній анімації. Розглянуто складові, які необхідно враховувати при виконанні завдань анімації, зокрема відмінності між інтерполяцією та апроксимацією кривих, складність інтерполяційних рівнянь та поняття гладкості кривої. Проаналізовано основні методи інтерполяції значень, серед яких лінійна, тригонометрична, кубічна та сферична.*

Ключові слова: *комп'ютерна графіка, анімація, інтерполяція значень, 3D-візуалізація.*

Більшість ранніх систем комп'ютерної анімації використовували механізм ключових кадрів [1–3]. Анімація у таких системах здійснювалася у двовимірному просторі та використовувався принцип, коли головні аніматори створювали основні ключові кадри, а їх асистенти відповідали за рисування проміжних кадрів для заповнення пробілів між ключовими кадрами анімації. Ключові кадри, у такій методиці створювалися досить часто, що дозволяло чітко визначати проміжні рухи анімації.

Пізніше у комп'ютерній анімації поняття "ключовий кадр" було розширено, що дало можливість анімувати будь-яку змінну, основне значення якої задається в певні ключові моменти анімації, а значення для проміжних кадрів обчислюються за допомогою інтерполяції. Такі системи називаються трековими, а змінні ключових кадрів – "articulation variables" [4]. Спрощений інтерфейс часової шкали для інтерполяції значень ключових кадрів подано на рисунку 1. Одними із перших тривимірних систем де використовувалися механізми ключових кадрів є TWIXT [5] та ВВОР [6]. Оскільки ці анімаційні системи наслідують методи двомірної анімації, основна операція полягає в інтерполяції між кривими – як замкнутими, так і розімкнутими.

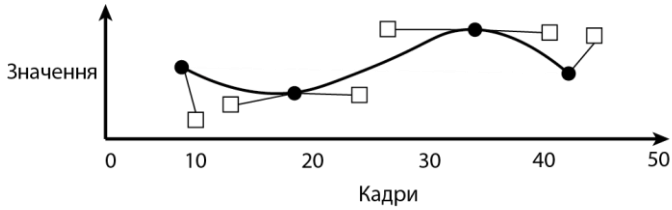


Рисунок 1 – Зразок інтерфейсу часової шкали
в комп'ютерних анімаційних системах

Системи комп'ютерної анімації побудовані на принципах інтерполяції значень. Така інтерполяція вимагає наявність крайніх значень, між якими треба заповнити проміжні значення. Простий приклад використання інтерполяції в анімації – це зміна позиції точки у просторі. Інтерполяція є набором методів для поступового перетворення одного числового значення в інше. Отримана послідовність чисел може використовуватись для трансформації, масштабування, обертання об'єкта, переміщення віртуальної камери, або зміни параметрів, таких як позиція, колір або яскравість джерела світла та інші. Зазвичай аніматор задає список значень для певного параметра на ключових кадрах, і виникає проблема, як оптимально обчислити значення параметра для кадрів між ключовими. *Наприклад*, якщо на одному кадрі положення об'єкта дорівнює координатам (0, 0, 0), а на іншому кадрі (10, 10, 10), потрібно визначити проміжні значення між цими кадрами. Для такого завдання може використовуватися лінійна інтерполяція. Проте, якщо об'єкт на одному кадрі має розпочинати рух із прискоренням, і зупинятися на іншому із деяким гальмуванням, то потрібно буде використовувати більш складнішу інтерполяцію.

При виконанні завдань анімації потрібно врахувати такі аспекти як: вибір інтерполяційної функції, параметризація функції та складність інтерполяційного рівняння. При роботі з набором точок, що описують криву, є вибір між інтерполяцією та апроксимацією значень. Вибір залежить від того, чи повинна крива проходити через задані точки у випадку інтерполяції, або ж ці точки лише задають форму кривої без необхідності прямого проходження через них, у випадку апроксимації. Якщо крива точно проходить через усю вибірку точок використовується інтерполяційний сплайн. У випадку апроксимації застосовуються апроксимуючі сплайни, що дозволяють змінювати форму кривої шляхом маніпуляції контрольними точками. Серед найпоширеніших інтерполяційних функцій – сплайни Герміта і Катмулла-Рома. Сплайн Герміта потребує інформації про доти-

чні в його крайніх точках, тоді як сплайн Катмулла-Рома використовує лише позиції, через які має проходити крива. До апроксимуючих функцій належать криві Безьє та B-сплайни, які можуть апроксимувати частину або всі контрольні точки.

Складність інтерполяційного рівняння впливає на ефективність процесу анімації, тому чим простіше інтерполяційне рівняння, тим швидше його можна обчислити. Поліноми вищих ступенів зручні в обчисленнях та забезпечують необхідну гнучкість керування анімованим значенням. Поліноми нижчих ступенів не дозволяють створити точку перегину між кінцевими точками, що обмежує їх застосування в деяких випадках, і як правило потребують більше обчислювальних ресурсів. Гладкість – це параметр, який визначає форму кривої та її поведінку. Математично гладкість визначається рівнем безперервності похідних від рівняння кривої. Безперервність нульового порядку вказує на неперервність значень самої кривої. Якщо при малих змінах параметра крива змінюється незначно, вона має нульовий, або позиційний порядок безперервності. Перший порядок безперервності передбачає неперервність першої похідної функції, що забезпечує тангентну безперервність. Другий порядок відповідає плавній зміні дотичного вектора. В геометричному дизайні часто використовують безперервність другого порядку для кривих і поверхонь, але в анімаційних системах для просторових кривих зазвичай достатньо безперервності першого порядку. Водночас для кривих, що описують залежності часу від відстані, інколи необхідно скористатись безперервністю другого порядку.

До найбільш розповсюджених методів інтерполяції значень для анімації ключових кадрів відносять: лінійну, тригонометричну, кубічну, сферичну.

Лінійна інтерполяція – це метод підгонки кривої за допомогою лінійних поліномів для побудови нових точок даних у діапазоні дискретного набору відомих точок даних, що забезпечує рівномірний розподіл значень між інтерпольованими точками.

Формула лінійної інтерполяції (1) є найпростішим підходом для визначення значення функції між двома відомими значеннями. Окрім цього метод корисний для апроксимації кривої за допомогою лінійних поліномів.

$$n = n_1 + t(n_2 + n_1), \qquad (1)$$

де n_1, n_2 – початкове та кінцеве значення інтерполювання; $0 \le t \le 1$ – параметр кроку інтерполяції.

Лінійний метод інтерполяції забезпечує, що рівні зміни параметра *t* відповідають рівним змінам в інтерпольованих значеннях. Однак інколи виникає потреба, щоб рівномірні кроки в *t* приводили до нерівномірних змін інтерпольованих значень. Реалізувати такий процес можна за допомогою ма-

тематичних підходів, таких як тригонометричні функції або поліноми. У загальному випадку тригонометричний підхід описується рівнянням (2).

$$n = n_1 \cos^2(t) + n_2 \cos^2(t), \qquad (2)$$

де $0 \le t \le \frac{\pi}{2}$ – діапазон інтерполяції.

Головний недолік такого підходу полягає в тому, що неможливо змінити характер кривої, тобто вона залишається синусоїдальною, а її нахил залежить від інтерпольованих значень. Один із способів отримати більший контроль над формою інтерпольованої кривої є застосування поліному третього ступеня (3), що описує кожен інтерполяційний сегмент.

$$V = at^3 + bt^2 + ct + d, \qquad (3)$$

де a, b, c, d – коефіцієнти, що визначають форму кривої між двома точками.

Кубічна інтерполяція – це метод, який використовується для побудови гладких кривих, що проходять через або поблизу заданих точок, за допомогою поліномів третього ступеня. На відміну від лінійної або квадратичної інтерполяції, які можуть не забезпечувати плавності на стиках між сегментами, кубічна інтерполяція дозволяє досягти більшої гладкості і забезпечує безперервність як першої, так і другої похідних між сегментами.

Коефіцієнти кубічного полінома зазвичай обчислюють за допомогою систем рівнянь, де враховують значення функції та її похідні в точках інтерполяції. Застосування кубічної інтерполяція гарантує гладкість на стиках між сегментами завдяки тому, що перші та другі похідні є безперервними. Це означає, що крива не буде містити різких змін у нахилах між точками.

Інтерполяція кватерніонів – це техніка для плавної зміни орієнтації в тривимірному просторі. Кватерніони є альтернативою до традиційних методів обертання, таких як матриці або Ейлерові кути. При інтерполяції кватерніонів використовується метод сферичної лінійної інтерполяції (SLERP). Кватерніон $q = (w, x, y, z)$ представляє обертання в 3D-просторі. Якщо є два кватерніони q_1 та q_2, які представляють початкове і кінцеве обертання, то для визначення проміжного значення кута повороту в момент часу *t*, можна використати рівняння сферичної інтерполяції, що записується як:

$$S(q_1, q_2, t) = \frac{\sin((1-t)\theta)}{\sin\theta} q_1 + \frac{\sin(t\theta)}{\sin\theta} q_2, \qquad (4)$$

де θ – кут між кватерніонами $q_1, q_2; t \in [0;1]$ – інтерполяційний коефіцієнт.

Використання такого методу забезпечує плавний перехід між початковим і кінцевим обертаннями та гарантує, що кутовий рух відбувається вздовж найкоротшого шляху на 4D-сфері, яка описує кватерніонний простір. SLERP забезпечує рівномірну кутову швидкість, що особливо важливо в анімації, оскільки це створює природний і рівномірний рух.

Висновки. Таким чином, комп'ютерна анімація ґрунтується на використанні різних методів інтерполяції або апроксимації, вибір яких залежить від бажаних властивостей анімації.

Інформаційні джерела

1. Burtnyk N., Wein M. Computer Generated Key Frame Animation. Journal of the Society of Motion Picture and Television Engineers. – 1971. – №8(3). – С. 149–153.

2. Burtnyk N., Wein M. Interactive Skeleton Techniques for Enhancing Motion Dynamics in Key Frame Animation. Communications of the ACM. – 1976. – №19(10). – С. 564–569.

3. Catmull E. The Problems of Computer-Assisted Animation / Catmull. // ACM SIGGRAPH Computer Graphics. – 1978. – №12(3). – С. 348–353.

4. May S. Encapsulated Models: Procedural Representations for Computer Animation. Ph.D. dissertation. Ohio State University – 1998.

5. Gomez J. Twixt: A 3D Animation System / Gomez. // Computers & Graphics. – 1985. – №9. – С. 291–298.

6. Stern G. BBOP–A program for 3-dimensional Animation / Stern. // Nicograph 83 proceedings. – 1983. – С. 403–404.

Напрям 15

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРОЄКТАМИ

UDC 004.8

SUBJECTIVE PERCEPTION MODEL OF SOFTWARE SUPPORT, ENCAPSULATED WITH A MULTILAYER PERCEPTRON

Andrii PUKACH
Vasyl TESLYUK
Lviv Polytechnic National University, Lviv, Ukraine.

Анотація*. Робота присвячена розробленню моделі суб'єктивного сприйняття підтримки програмних продуктів за допомогою інкапсуляції відповідних штучних нейронних мереж типу багатошарового перцептрона. Розроблена модель дає змогу здійснити представлення та дослідження факторів впливу, що впливають на суб'єктивізацію сприйняття підтримуваних програмних продуктів та/або процесів їх комплексної підтримки, з метою забезпечення подальшої можливості автоматизації цієї підтримки.*

Ключові слова*: автоматизація, фактори впливу, модель суб'єктивного сприйняття, підтримка програмних продуктів, багатошаровий перцептрон, штучні нейронні мережі.*

Abstract. *A subjective perception model of software support, encapsulated with multilayer perceptron artificial neural networks, is developed, which makes possible to investigate impact factors affecting the perception's subjectivization of the supported software and/or processes of its comprehensive support with the aim of ensuring further possibility of its automation.*

Keywords*: automation, impact factors, subjective perception model, software support, multilayer perceptron, artificial neural networks.*

Introduction. One of the most urgent scientific and applied problems nowadays is the problem of automation of complicated and complex processes, including the processes of software complexes' support. This problem includes many specific scientific and applied tasks, one of which is the task of analyzing the impact factors which influence the results of perception of the supported object (that could be the supported software complex itself, as well as the processes of its comprehensive support) by the relevant subjects of interaction with this object. In fact, the main scientific and applied task considered in this paper is ensuring the possibility of

developing a sufficiently simple, clear and concise, but at the same time maximally unified and universal, model for representation and further research of the processes (and results) of perception subjectivization of any researched object or process (in general case), as well as researched software complexes (in the context of the above-mentioned scientific and applied problem of software complexes support automation). In particular, based on the researches presented in works [1–12], the main directions of automation in the context of software complexes comprehensive support, are further examples, like: software testing automation; development and operations (DevOps) automation; automation of information technologies (IT) incident processing, and others related to comprehensive support of any software products. However, all of them represent only partial cases of the investigated area. That's why there is a need to develop a more generalized model, which would, in fact, provide possibilities for modeling the processes of subjective perception of investigated supported objects (or processes) by relevant subjects of interaction with these objects (or processes).

Generalized model for describing subjective perception of the supported objects (software complexes). Let's start with this generalized model of subjective perception of the supported objects. Before encapsulation of any artificial intelligence (AI) component(s), like a multilayer perceptron (MP) artificial neural networks (ANN), it is necessary to develop a generalized model of subjective perception of the supported objects. The representation format (or form) of such a generalized model can be completely arbitrary. However, it obviously must contain and reflect following key elements like:

– input characteristics of the researched object (the supported software complex, or processes of its comprehensive support);

– a list of identified impact factors affecting the results of subjective perception of this object by relevant subjects interacting with it;

– absolutely all impact factors present in the model must be: clear, clearly defined, consistently structured, and their impact must be known and defined;

– output characteristics that unambiguously interpret the result(s) of object's perception by the relevant interaction subject;

– the model should reflect real processes of transformation of object's input characteristics into the relevant output ones through the mediation of impact factors.

Fig. 1 below presents an example of a generalized model of subjective perception of the supported software complex.

Encapsulation of ANN into a generalized model. The next stage after the development of a supported software complex's subjective perception generalized model – is actually the encapsulation of the neural network (of a certain type, not only BP, but any other as well, depending on requirements) into the resulting generalized model. The main task of ANN encapsulating into the developing finalized model of supported software complex's subjective perception – is to comply with one single, simple and clear, but extremely important and mandatory

unambiguous criterion: the encapsulated ANN should as correctly as possible reflect the processes of transformation of input characteristics by impact factors, and guarantee obtaining corresponding resulting characteristics (according to the represented generalized model, and in accordance with the data for further training and testing of used ANN).

Ensuring the ability of identifying impact factors. The final stage (and task at the same time) of development a supported software complex's subjective perception model – is to ensure the possibility of identifying impact factors. For this reason appropriate mathematical model for analysis the influence of impact factors onto the software complexes' support is used, represented in research [13]. Fig. 2 below represents obtained example results of ensuring the identification of impact factors of the subjective perception model with encapsulated trained MP ANN.

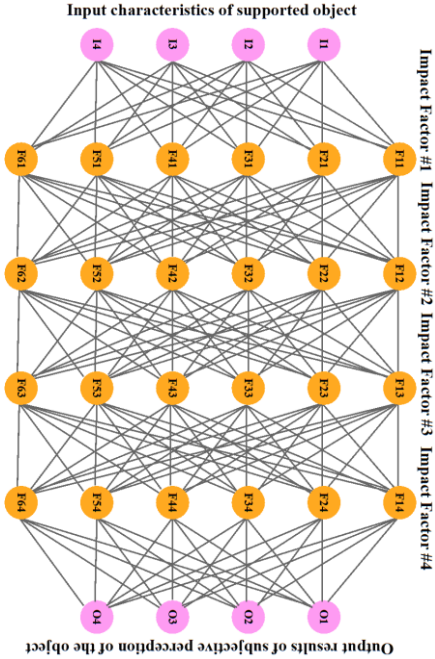


Figure 1 – Example of a generalized model of the supported software complex's subjective perception

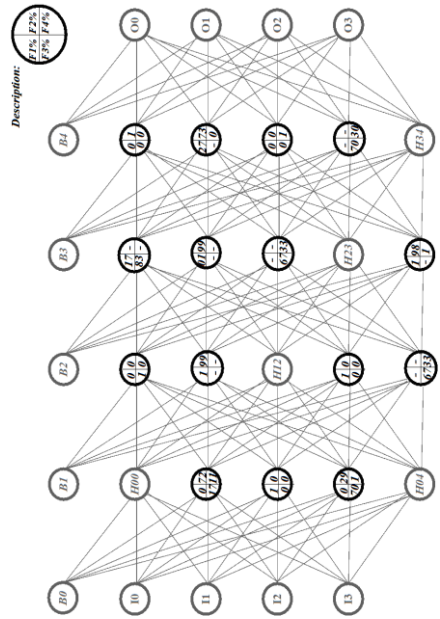


Figure 2 – Example results of ensuring the identification of impact factors of the subjective perception model with encapsulated MP ANN

Therefore, in case of using MP type as an ANN encapsulated into a model of subjective perception of the supported object, it is necessary to ensure the

following steps to correctly represent the processes of subjective perception of the supported object, caused by relevant impact factors:

– the input layer of MP neurons will interpret the input characteristics of the object;

– the output layer of MP neurons will interpret the resulting output characteristics of subjective perception of this object;

– hidden layers of MP neurons will interpret impact factors. At the same time, the number of hidden layers of encapsulated MP should be such that could:

– ensure all appropriate necessary MP requirements for its training parameters (accuracy, speed, and other additional) as well as its further testing;

– ensure further possibility of unambiguous identification of various separate impact factors.

Conclusions. This paper is devoted to development of the subjective perception model of software complexes support objects (which are: supported software complexes themselves, as well as processes of their comprehensive support), with encapsulation of a MP ANN. It ensures the possibility for developing a sufficiently simple, clear and concise, but at the same time maximally unified and universal, model for representation and further research of the processes (and results) of perception's subjectivization of any researched object or process (in general case), as well as researched software complexes in the context of global scientific and applied problem of software complexes support automation.

Information sources

1. Abhilash R., Pabbath R. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. NeuroQuantology, 19(12), pp. 764–773. URL: https://doi.org/10.48047/nq.2021.19.12.NQ21280

2. Ahmed S., Singh M., Doherty B., Ramlan E., Harkin K., & Coyle D. (2023). AI for Information Tecchnology Operation (AIOps): A Review of IT Incident Risk Prediction. In 2022 9th International Conference on Soft Computing and Machine Intelligence (ISCMI 2022). IEEE, Advance online publication, pp. 253–257. URL: https://doi.org/10.1109/ISCMI56532.2022.10068482

3. Ogala J. O. (February 2022). A Complete Guide to DevOps Best Practices. International Journal of Computer Science and Information Security (IJCSIS), 20(2), pp. 1–6. URL: https://doi.org/10.5281/zenodo.6376787

4. Krishna Neupane. (2023). Continuous Automation with DevOps practices for Threat Detection, 99 pages. URL: https://doi.org/10.13140/RG.2.2.33472.92169

5. Montvelisky J., Bhamare L. (2024). 11th edition of the State of Testing Report. Practi Test & Tea-time with Testers. URL: https://www.practitest.com/assets/pdf/stot-2024.pdf

6. Sumanth T. (2021). A Comprehensive Overview of DevOps and Its Operational Strategies. International Journal of Information Technology & Management Information System (IJITMIS), 12(1), pp. 15–32. URL: https://iaeme.com/MasterAdmin/Journal_uploads/IJITMIS/VOLUME_12_ISSUE_1/IJITMIS_12_01_002.pdf

7. Tatineni S. (2022). AI-Infused Threat Detection and Incident Response in Cloud Security. International Journal of Science and Research (IJSR), 12(11), pp. 998–1004. URL: https://dx.doi.org/10.21275/SR231113063646

8. Hamza U., Syed-Mohamad M., Nasuha S., Abdullah L. (2023). DevOps Adoption Guidelines, Challenges, and Benefits: A Systematic Literature Review. International Center for Research and Resources Development (ICRRD), 4(1), pp. 149–171. URL: https://doi.org/ 10.53272/icrrd

9. Thomson A. (2024). Proactive customer support: Re-architecting a customer support/relationship management software system leveraging predictive analysis/AI and machine learning. Engineering: Open Access, 2(1), pp. 39–50. URL: https://doi.org/ 10.33140/ eoa.02.01.04

10. Reinhard P., Wischer D., Verlande L., Neis N., Li M. M. (2023). Towards designing an AI-based conversational agent for on-the-job training of customer support novices. International Conference on Design Science Research (DESRIST), Pretoria, South Africa, 31 May – 02 Jun 2023, 15 p. URL: https://www.alexandria.unisg.ch/ handle/ 20.500.14171/107617

11. Inavolu S. M. (2024). Exploring AI-Driven Customer Service: Evolution, Architectures, opportunities, challenges and future directions. International Journal For Multidisciplinary Research, 6(3), 23 p. URL: https://doi.org/10.36948/ijfmr.2024. v06i03.22283

12. Salminen T. (2024). Possibilities of AI in customer care in the software business. Master's Thesis. Turku University of Applied Sciences Mechanical and Marine Engineering, 2024, 76 p. URL: https://urn.fi/URN:NBN:fi:amk-202404298185

13. Pukach A. I., & Teslyuk V. M. (2024). Mathematical model for analysis of influencing factors on software complexes support. Printing and Publishing, 1(87), pp. 75–85. URL: https://doi.org/10.32403/0554-4866-2024-1-87-75-85

UDC 338.28

RISK MANAGEMENT OF CYBER PROTECTION PROGRAMS FOR CRITICAL INFRASTRUCTURE FACILITIES

Oleh KOVALCHUK
Roman RATUSHNYI
Lubov PERETYATKO
Ivan ZHUK

Department of Law and Management in Civil Protection, Lviv State University of Life Safety.

Анотація. *Зі стрімким впровадженням новітніх інформаційних технологій у всі сфери діяльності збільшується і кількість цінної інформації, від безпеки якої залежать об'єкти інфраструктури. Об'єкти критичної інфраструктури, такі як: електростанції, транспортні системи, медичні установи, банки та інші системи у своїй діяльності використовують різні системи підтримки прийняття рішень та інформаційні системи, в яких недостатня кібернетійкість може призвести до серйозних наслідків.*

Ключові слова: *інформаційна безпека, ризик менеджмент, інформаційні системи, інфраструктура.*

Abstract. *With the rapid implementation of the latest information technologies in all spheres of activity, the amount of valuable information on the security of which critical infrastructure facilities depend on is also increasing. Objects of critical infrastructure, such as: power plants, transport systems, medical institutions, banks and other systems in their operations require various decision support systems and information systems, in which a lack of cyber security can lead to serious consequences.*

Keywords: *information security, risk management, information systems, infrastructure.*

Successful managers skillfully analyze risks and make informed decisions relying on competence and experience. Managers have to consider many external and internal organizational factors that influence uncertainty. Risk management is an iterative process, the purpose of which is to ensure the achievement of the organization's goals. The process of improving the management system of state critical facilities should take into account the best practices of risk management. To optimize these processes, managers use information technologies such as corporate information and ERP systems. They enable efficient management of infrastructure projects, programs and project portfolios (Fig. 1).

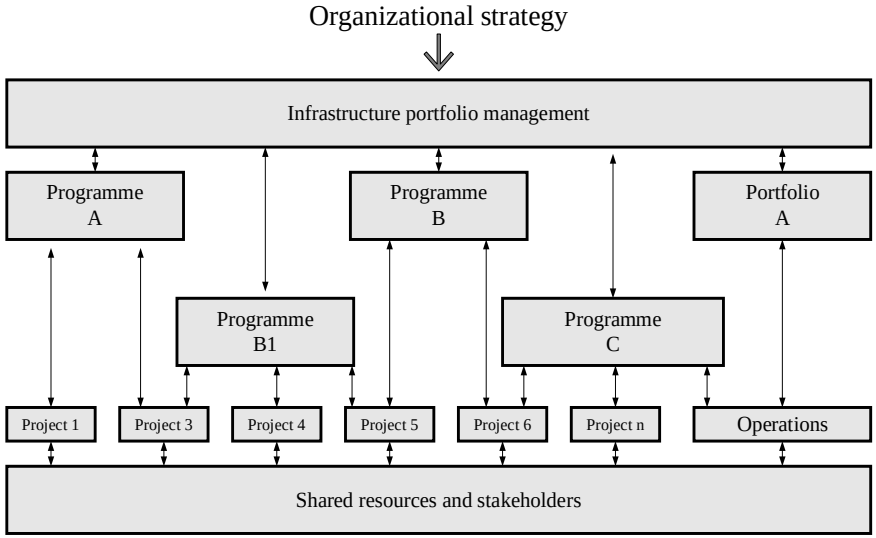


Figure 1 – A portfolio of critical infrastructure consisting of various components

Objects of critical infrastructure, such as: power plants, transport systems, medical institutions, banks and other systems in their activities use various decision

support systems and information systems in which insufficient cyber resistance can lead to serious consequences. Ishikawa and BTA – Bow-Tie Analysis methods are used to analyze causal relationships in risk management. Managing risk is based on the principles, framework and process outlined in (Fig. 2) [6].

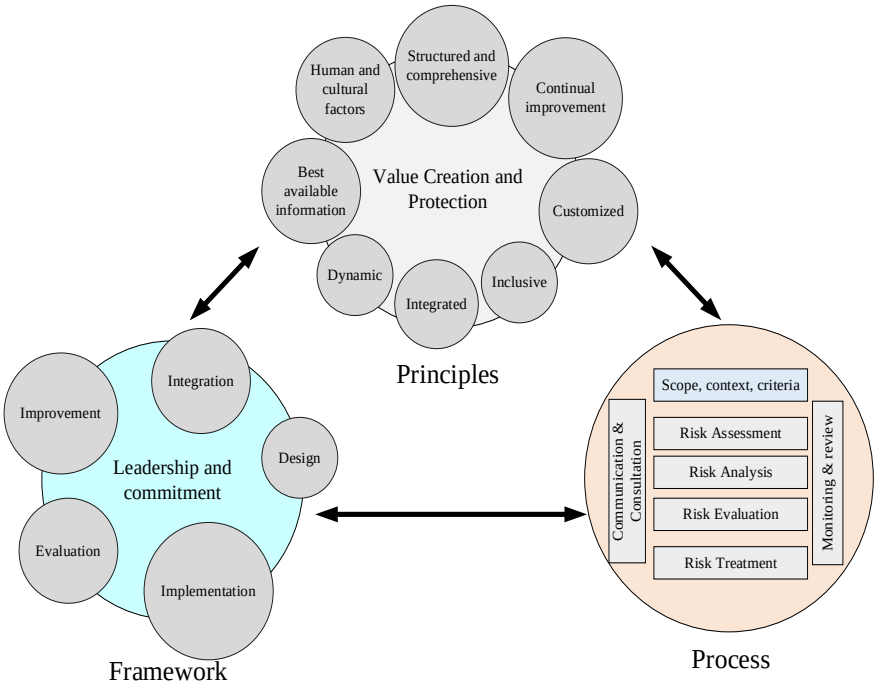


Figure 2 – Principles, framework and process efficient risk management

The characteristics of risk management may differ significantly depending on the chosen strategy. For example, a proactive approach involves constant monitoring of risks and the development of preventive measures, while a reactive approach focuses on eliminating the consequences of problems that have already occurred. The choice of risk management strategy directly affects the structure and functions of risk management programs. Some strategies require the creation of dedicated units responsible for risk management, while others may involve the division of responsibilities among different divisions of the organization. The effectiveness of risk management depends on the extent to which the chosen strategy corresponds to the specifics of the organization and the nature of the risks it faces. There is no one-size-fits-all strategy that fits all organizations.

Table 1.

Characteristics of risk management depending on strategic approaches to formation risk management programs

Characteristics risk-management	*A strategic approach to forming a risk management program*			
	Conservative	*Maximizer*	*Manager*	*Pragmatist*
Management goals risks	Loss control. Software system security	Reward for accepted risks. Profit from purchase or sale of risks	Impact on risks by means of a series of measures	Diversification. Avoidance of large risk concentrations
Strategic orientation risk-management	Low risk-appetite. Minimization risks with a goal minimization losses Stabilization results	High risk-appetite. Maximization increase profit for maximum (accepted) risks	Average risk-appetite. Strategic decision, aimed at increase cost	Strategic benefits relate to receiving benefits from the complex different, maybe not related risks
Features management risks	Hard limits, restrictions and regulators. Control over commercial bank operations or insurance companies	Flexible opportunities	Formal politicians and standards	Flexible options, high degree communications and competencies. Portfolio management risks
Approaches to analysis and assessment risks	Stress testing. Analysis sensitivity Scenario analysis.	Models pricing, methods rating agencies. Evaluation and reservation trade operations banking and insurance activity	Economic capital and added cost. Reward for risk and budgeting	Simplified economic capital
Reports from management risks	Compliance limits Impact on risks, that arose	Correlation profit and risks that related to him	Coefficient profitability equity, risk budget	Concentration of risks: arising losses due to large positions in one asset or on a certain market. Consolidated report about risks
Environment dominance risk	Collapse	Lift	Discreet	Indeterminate

Conclusions. Therefore, to increase the cyber security of the energy system, it is necessary to apply a comprehensive approach, which includes both technical measures (updating software, intrusion detection systems) and organizational measures (increasing staff awareness, developing incident response plans). International cooperation and exchange of experience also play an important role.

Information sources

1. Shipovsky Volodymyr. System of indicators for assessing cyber resilience of information systems of critical infrastructure objects Information Protection, volume 25, number 1, January-March 2023, pp. 37–45. doi: 10.18372/2410-7840.25.17597.

2. Kovalchuk Oleh, Kobylkin Dmytro and Zachko Oleh. Graphodynamic modeling for a multi-agent support system for personnel decision-making in the field of human safety. Proceedings of the 4th International Workshop IT Project Management (ITPM 2023). Warsaw 2023, pp. 149–159.

3. Kovalchuk O., Kobylkin D. and Zachko O. "HR Decision-Making Support System Based On The CBR Method", 2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT), Lviv, Ukraine, 2023, pp. 1–4. doi: 10.1109/ CSIT61576.2023.10324169.

4. Kovalchuk Oleh, Zachko Oleg. Models of the life cycle of forming project teams in a security-oriented system IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), IWPM 2020, 2, pp. 211–214, 9321932. doi:10.1109/ CSIT49958.2020.9321932.

5. ДСТУ ISO 21503:2022 "Project, programme and portfolio management – Guidance on programme management".

6. ISO 31000:2018 Risk management – Guidelines.

7. IPMA Organisational Competence Baseline (IPMA OCB). IPMA, 2013, 67 p.

УДК 004.4

ПРОЕКТУВАННЯ ІНТЕРАКТИВНОЇ СИСТЕМИ УПРАВЛІННЯ ГОТЕЛЬНИМ БІЗНЕСОМ ЗА ДОПОМОГОЮ UML-ДІАГРАМ

Валерія МІДЯНКА

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract*. The purpose of this work is the methodological development and practical implementation of an interactive hotel business management system using UML diagrams to model the architecture, processes, and interactions between system components. This allows for effective automation of key business processes in the hotel sector, such as reservation management, customer accounting, financial monitoring, and reporting, as well as integration with modern technologies to increase the competitiveness of the hotel enterprise.*

Keywords*: information system, hotel, UML models, use case diagram, activity diagram.*

Анотація*. Метою цієї роботи є методичне опрацювання та практична реалізація інтерактивної системи управління готельним бізнесом із використанням UML-діаграми для моделювання архітектури, процесів і взаємодії між компонен-*

тами системи. Це дозволяє забезпечити ефективну автоматизацію основних бізнес-процесів у готельному секторі, таких як управління бронюванням, облік клієнтів, фінансовий моніторинг та формування звітності, а також інтеграцію із сучасними технологіями для підвищення конкурентоспроможності готельного підприємства.

Ключові слова: *інформаційна система, готель, UML моделі, діаграма прецедентів, діаграма діяльності.*

У наш час автоматизоване управління організацією є обов'язковою частиною сучасних принципів керівницької діяльності. В сучасному світі інформаційних технологій важко знайти організацію, яка хоча б частково не була б автоматизована. Зберігання документів, клієнтської бази, а також інформації необхідної для безперебійної роботи компанії вимагає суттєвих витрат, як тимчасових так і грошових.

Предметною областю даної роботи є розробка інформаційної системи для управління готельним бізнесом. Інформаційна система, яка використовується в готельній справі має забезпечувати:

– достовірність і повноту інформації, яка міститься в ній;

– швидкість роботи, яка відповідає критеріям обслуговування;

– зв'язки між різними категоріями працівників організації;

– автоматизацію інформації, що передається дочірнім службам.

Для підтримки достовірності і повноти даних в інформаційній системі, треба контролювати правильність і коректність інформації, що вводяться користувачем, а також своєчасне їх корегування.

Швидкість роботи залежить як від швидкості виконання запитів до бази даних, так і від навичок роботи користувача ІС. Для прискорення навчання користувача необхідно щоб інформаційна система мала зрозумілий інтерфейс, а так само коректно складений посібник користувача. Залежно від займаної посади програмне забезпечення буде видавати доступ до відповідних функцій, які необхідні для виконання своїх зобов'язань, це так само допоможе в швидкості роботи користувача інформаційної системи.

Use Case – це техніка, яка використовується при розробці програмного забезпечення чи інформаційної системи для охоплення функціональних вимог даної системи, Use Case описує взаємодії, що відбуваються між "акторами" – ініціатором взаємодії самої системи з існуючими системами, варіант використання представлений простою послідовністю кроків.

Сам USE CASE описує систему, системне середовище та взаємозв'язок між системою та її середовищем. Опис послідовного набору дій, виконуваних системою, що призводить до появи значення для конкретного актора.

Use Case використовується для впорядкування поведінкових речей у моделі. Варіанти використання реалізуються у співпраці.

Діаграма прецедентів для інформаційної системи управління готельним бізнесом зображено на рисунку 1.

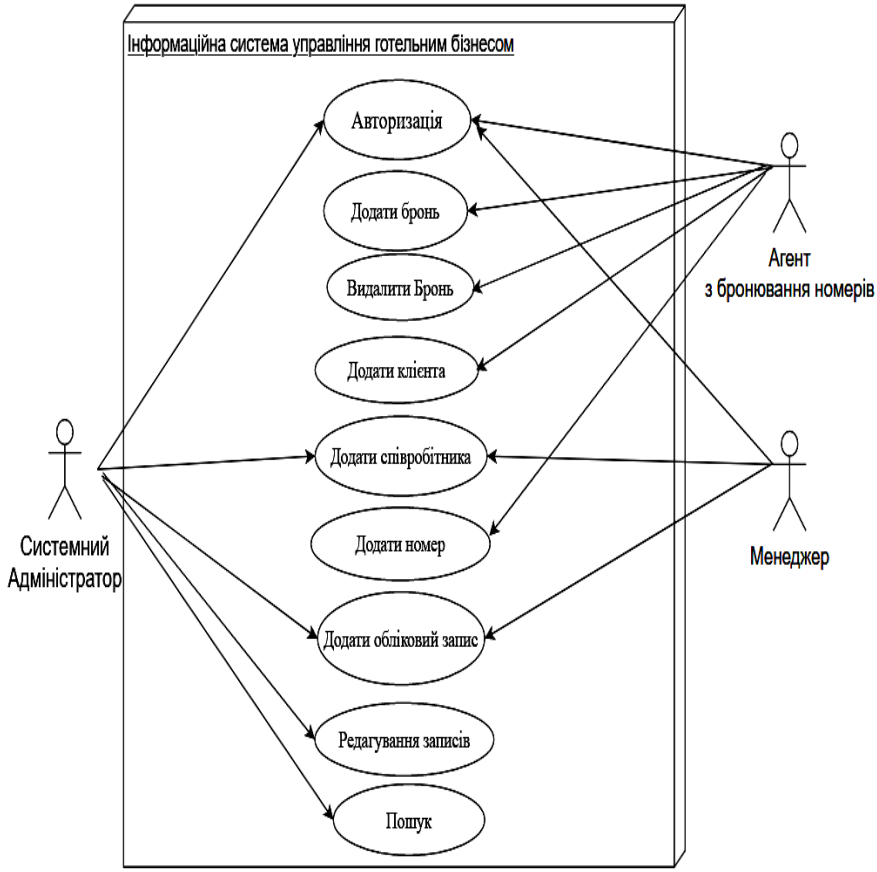


Рисунок 1 – Діаграма прецедентів ІС “управління готельним бізнесом”

Діаграми діяльності в основному описують різні потоки діяльності, які будуть розроблені в системі. Де кожен потік має початок, рішення, яке може відбутися в системі, і кінець у системі. Діаграми діяльності в основному мають структуру, яка майже схожа на блок-схему або блок-схему в структурованій системі. Ця діаграма діяльності складається на основі варіанту використання або декількох випадків використання у схемі випадків використання (рис. 2).

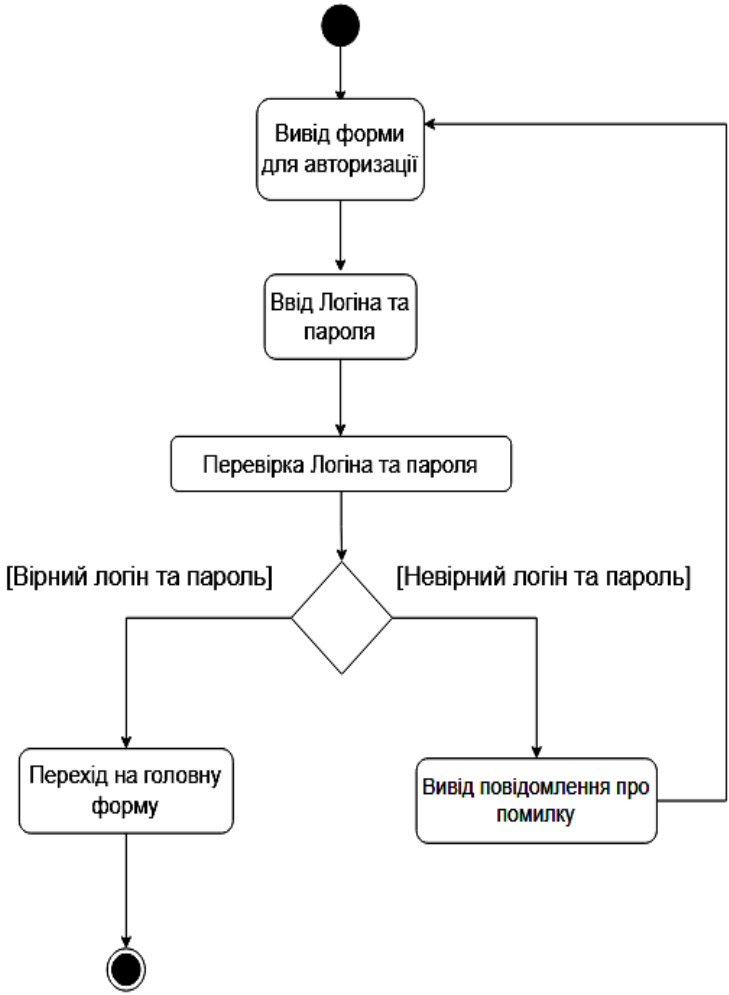


Рисунок 2 – Діаграма діяльності для форми авторизації користувачів інформаційної системи

Інформаційні джерела

1. Системи автоматизації готелів. URL: https://tourlib.net/statti_ukr/gudzovata.htm
2. Використання діаграм прецедентів та діяльності. URL: https://medium.com/@andrerahardjo/use-case-diagram-dan-activity-diagram-2b30f4471613

УДК 004.42

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ОБЛІКУ ПРОЄКТНОЇ ДІЯЛЬНОСТІ

Ірина ДЕЛІЖАН
Євгенія СОКОЛОВА
Національний аерокосмічний університет імені М. Є. Жуковського "Харківський авіаційний інститут", м. Харків, Україна.

Abstract*. Accounting for project activities is essential for managing a software developer firm. Successful implementation of projects requires careful planning, organization, control, and analysis of each stage. In this context, project accounting software becomes an indispensable tool that helps automate and optimize these processes.*
Keywords*: software, project accounting, WPF, XAML, C#, Microsoft SQL Server.*

Анотація*. Облік проєктної діяльності є важливим аспектом управління фірмою – розробником програмного забезпечення. Успішне виконання проєктів потребує ретельного планування, організації, контролю та аналізу кожного етапу. У цьому контексті програмне забезпечення для обліку проєктної діяльності стає незамінним інструментом, який допомагає автоматизувати та оптимізувати ці процеси.*
Ключові слова: *програмне забезпечення, облік проєктної діяльності, WPF, XAML, C#, Microsoft SQL Server.*

Програмне забезпечення обліку проєктної діяльності надає можливість відстежувати терміни виконання проєктів, ефективність команд. В умовах сучасного швидкозмінного ринку, де вимоги до якості та швидкості розробки постійно зростають, застосування таких систем дозволяє компаніям залишатися конкурентоспроможними та ефективно керувати своїми проєктами [1]. Розроблюване програмне забезпечення дозволить фірмам – розробникам програмного забезпечення досягати своїх бізнес – цілей, що наведені в табл. 1 з максимальною ефективністю.

Таблиця 1.

Бізнес – цілі розробки програмного продукту

Ідентифікатор	*Бізнес – цілі*
BC-01	Збільшити кількість успішно завершених проєктів на 20% за рахунок впровадження моніторингу статусів проєктів.
BC-02	Підвищити продуктивність роботи команди на 10% за рахунок аналізу витрат часу на різних етапах проєкту.

Виділено п'ять типів користувачів програмного забезпечення: "неавторизований користувач", "працівник", "керівник проєкту", "адміністратор" та

“керівник фірми”. Побудовано діаграму варіантів використання (рис. 1), що описує зв’язки між дійовими особами та варіантами використання, які у свою чергу відображають взаємодії між головною дійовою особою, рішенням та вторинними дійовими особами.

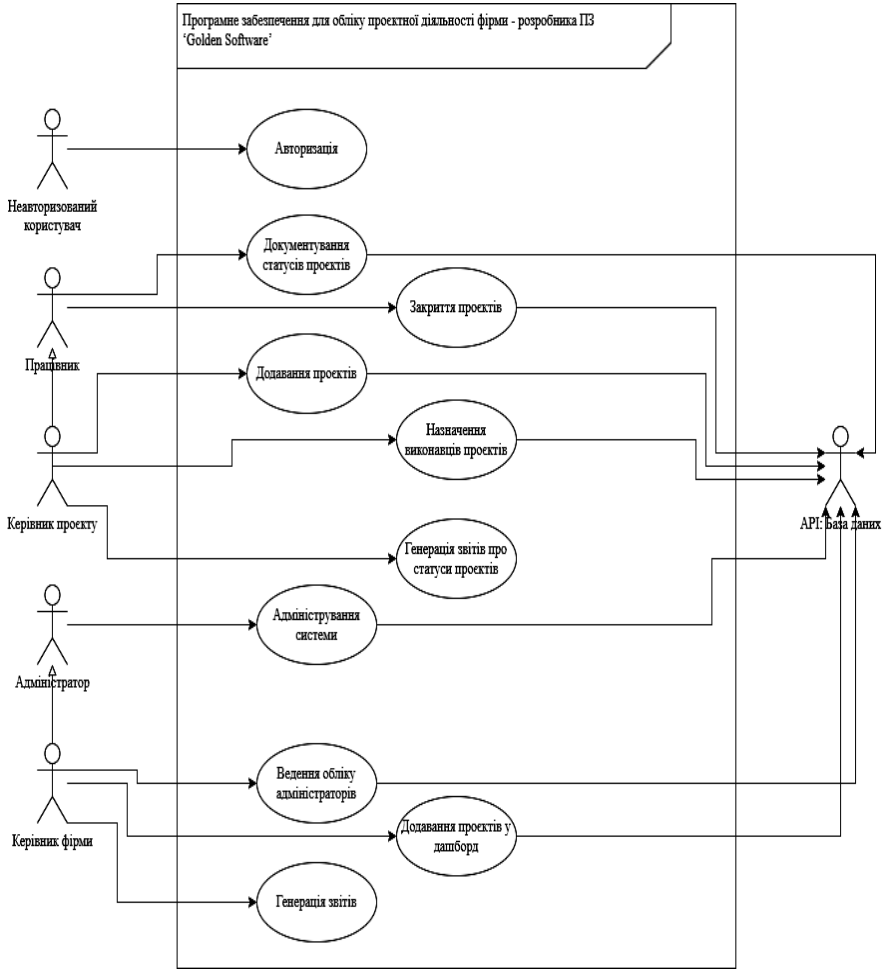


Рисунок 1 – Діаграма варіантів використання

Неавторизований користувач може авторизуватись; працівник – виконувати проєкти й документувати їх статуси; керівник проєкту – додавати проєкти, призначати виконавців і генерувати звіти; адміністратор – адмініс-

трувати систему; керівник фірми – обліковувати адміністраторів, додавати проєкти у дашборд і генерувати звіти. Дані передаються через API, що забезпечує взаємодію з базою даних, чітко розмежовуючи права доступу.

На основі цих функціональних можливостей визначено два привілейовані класи користувачів: “адміністратор” – має доступ до управління працівниками та проєктами, може додавати, редагувати та видаляти інформацію про працівників, проєкти і їх статуси; “керівник фірми” – має найширший доступ до функціоналу ПЗ, включаючи можливість перегляду, редагування та видалення інформації про працівників, проєкти, статуси, а також адміністраторів і доступ до звітів. Наступним етапом розробки програмного забезпечення є побудова дерева функцій (рис. 2) на основі групування вимог користувачів за ієрархією функцій, що відображає розбиття завдань цих функцій з точки зору їх взаємозв’язків. Поділ завдань за категоріями дозволяє легко адаптувати систему до потреб різних ролей користувачів, одночасно забезпечуючи контроль доступу та ефективне управління даними.

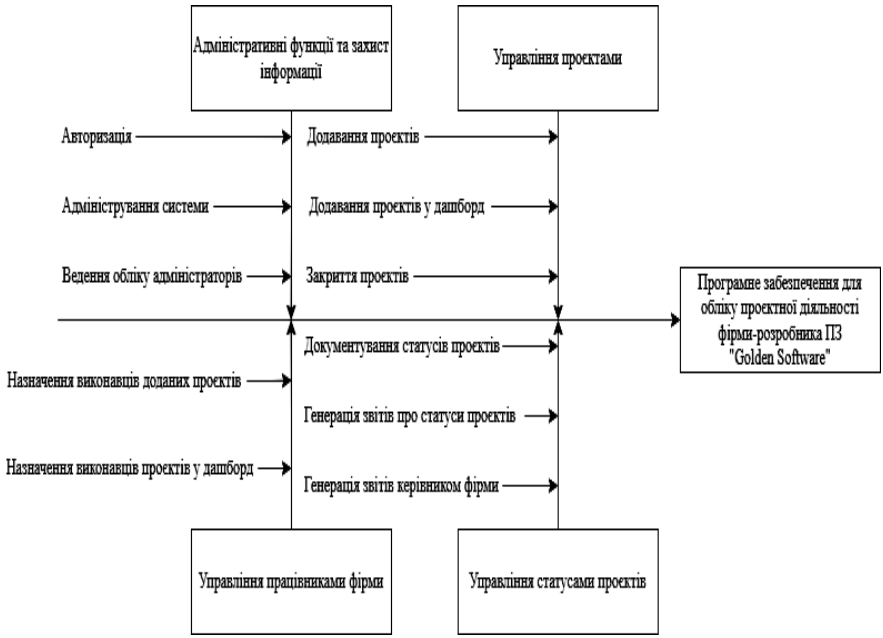


Рисунок 2 – Дерево функцій

На рисунку 3 наведено карту діалогових вікон, що ілюструє концепцію архітектури сторінок. Кожен прямокутник представляє вікно, яке братиме участь в операціях, описаних у варіантах використання. Вхід є центральною

точкою, що забезпечує доступ до вікон різних ролей користувачів, таких як “Вікно адміністратора” або “Вікно працівника”. Ця структура дозволяє забезпечити простоту взаємодії користувача із системою, водночас чітко розмежовуючи функціонал для різних типів користувачів. Така навігаційна схема забезпечує зручність і логічну послідовність при роботі з програмним забезпеченням. Для розробки програмного забезпечення з привабливим інтерфейсом обрано WPF із мовою XAML [2]. Для створення графіки використано пакет NuGet – MaterialDesignThemes. Функціональність реалізовано на C# – компактній та зручній для читання мові, що працює на платформі.NET [3]. Для збереження даних використано Microsoft SQL Server, оскільки програмне забезпечення розробляється для Windows 10.

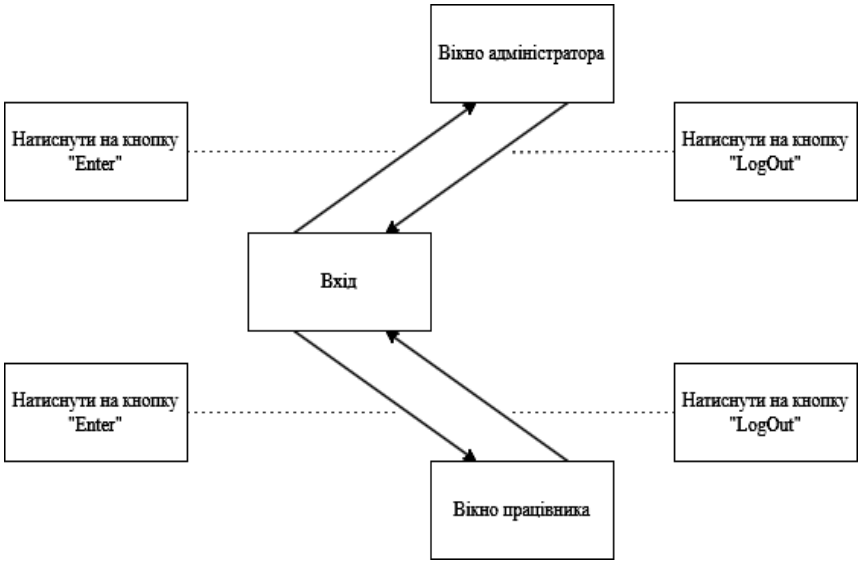


Рисунок 3 – Карта діалогових вікон

Висновки. Програмне забезпечення для обліку проєктної діяльності фірми – розробника ПЗ є ключовим інструментом для збереження інформаційної бази про працівників фірми, ведення журналу терміну роботи співробітників, ефективного управління проєктами та етапами їх розробки, відстеження термінів їх виконання з використанням реляційної бази даних Microsoft SQL Server. Таке ПЗ допомагає оптимізувати робочі процеси та підвищити продуктивність команди за рахунок функціональності, реалізованої мовою програмування C#, та інтуїтивно зрозумілого інтерфейсу, реалізованого за допомогою платформи WPF.

Інформаційні джерела

1. ДСТУ ISO/IEC/IEEE 16326:2015 Розроблення систем та програмного забезпечення. Процеси життєвого циклу. Керування проєктами (ISO/IEC/IEEE 16326:2009, IDT). URL: https://online. budstandart.com/ru/catalog/doc-page?id_doc=67052
2. Посібник із класичних додатків (WPF.NET). URL: https://learn.microsoft.com/ru-ru/dotnet/desktop/wpf/overview/ ?view=netdesktop-9.0
3. Що таке C#? URL: https://beetroot.academy/blog/shcho-take-c-chi-pidhodit-menicya-mova-programuvannya-chomu-vona-kruta

УДК 004.73:37.01

ВПЛИВ СОЦІАЛЬНИХ МЕРЕЖ НА ОСВІТНІЙ ПРОЦЕС: АНАЛІЗ ДАНИХ ЗА ДОПОМОГОЮ БІБЛІОТЕК PYTHON

Христина МЕЧУС
Ольга СМОТР

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract.*The study focuses on the impact of social media on the educational process of higher education students. Based on the analysis using Python, recommendations were developed for the effective use of social media in education. The study revealed a positive impact on resource accessibility and collaboration, as well as a negative impact due to distractions and misinformation.*

Keywords: *social media, education, Python, academic performance.*

Анотація. *Робота присвячена дослідженню впливу соціальних мереж на освітній процес здобувачів вищої освіти. На основі аналізу з використанням бібліотек Python розроблено рекомендації щодо ефективного застосування соціальних мереж у навчанні. Виявлено позитивний вплив на доступ до ресурсів і співпрацю, а також негативний – через відволікання та дезінформацію.*

Ключові слова: *соціальні мережі, освіта, Python, академічна успішність.*

Соціальні мережі стали невід'ємною частиною сучасного життя, суттєво впливаючи на всі аспекти суспільної взаємодії, включаючи освіту. Вони трансформували способи обміну інформацією, спілкування та самонавчання, відкривши нові можливості для здобувачів освіти. З одного боку, соціальні мережі надають доступ до безмежного обсягу інформації, дозволяють створювати професійні спільноти та забезпечують інтерактивність у навчальному процесі. З іншого боку, вони можуть відволікати, викликати залежність та навіть стати джерелом дезінформації [1, 2].

У цьому дослідженні я аналізую вплив соціальних мереж на освітній процес здобувачів вищої освіти, використовуючи інструментарій бібліотек Python для збору, обробки та візуалізації даних. Такий підхід дозволяє комплексно оцінити як позитивні, так і негативні аспекти взаємодії студентів із соціальними мережами.

Мета роботи полягає у вивченні впливу соціальних мереж на академічну успішність, мотивацію до навчання та емоційний стан здобувачів вищої освіти. Застосування бібліотек Python як основного інструмента аналізу даних дає змогу проводити глибокий аналіз великих обсягів інформації та отримувати статистично значущі висновки.

Для виконання завдань дослідження я використовувала набір бібліотек Python, зокрема:

– Pandas – для обробки та структурування даних;

– Matplotlib та Seaborn – для побудови візуалізацій;

– Plotly – для створення інтерактивних графіків.

Дані для аналізу були отримані з опитувань студентів, які охоплювали питання про час, витрачений у соціальних мережах, цілі використання платформ, а також їхній вплив на навчання [3, 4].

Позитивний вплив соціальних мереж:

Доступ до навчальних ресурсів: Більшість опитаних студентів (78%) зазначили, що використовують соціальні мережі для пошуку навчальних матеріалів, таких як відеолекції, статті та вебінари. Платформи на кшталт YouTube та LinkedIn значно сприяють самонавчанню.

Комунікація та співпраця: Соціальні мережі допомагають студентам координувати групові проєкти та обговорювати навчальні питання. *Наприклад*, 62% респондентів активно використовують групові чати для підготовки до іспитів.

Розширення професійних контактів: Завдяки платформам, як LinkedIn, студенти можуть будувати професійні зв’язки, що сприяє їхньому працевлаштуванню після завершення навчання.

Міжнародна взаємодія: Соціальні мережі дозволяють брати участь у глобальних дискусіях і приєднуватися до міжнародних конференцій, що стимулює кроскультурний обмін досвідом.

Негативний вплив соціальних мереж:

Відволікання: У середньому студенти витрачають до 3 годин на день на розважальний контент у соціальних мережах, що знижує їхню продуктивність. Аналіз даних показав кореляцію між збільшенням часу в соцмережах і зниженням середніх оцінок.

Дезінформація: 35% студентів вказали, що стикалися з неправдивою інформацією, яка вводила їх в оману під час підготовки до занять.

Соціальна ізоляція: Хоча соціальні мережі сприяють онлайн-взаємодії, вони часто замінюють живе спілкування, що може негативно впливати на психологічний стан студентів.

Психологічний тиск: 47% респондентів визнали, що постійне порівняння своїх успіхів із “ідеальними” профілями в соціальних мережах викликає у них стрес та знижує самооцінку.

Аналіз даних дозволив створити інформативні візуалізації, такі як:

1. Графік залежності часу, проведеного в соціальних мережах, від академічної успішності:

Він показує негативну кореляцію (r = –0.47). Чим більше часу студент витрачає на соціальні мережі, тим нижча його академічна успішність. Лінія тренду на графіку ілюструє цей зв’язок.

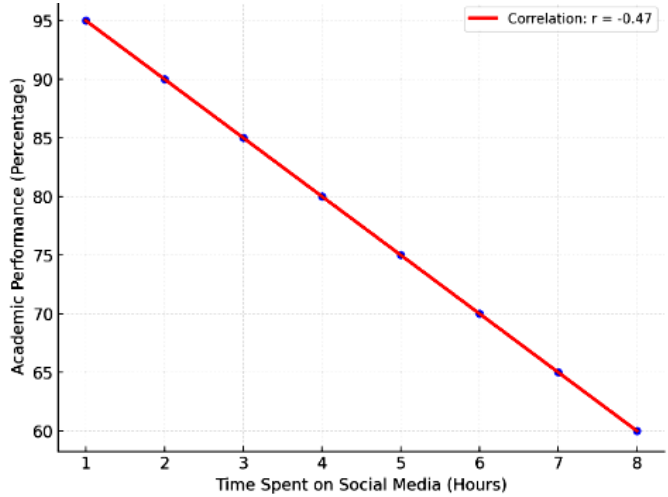


Рисунок 1 – Графік залежності

2. Інтерактивна кругова діаграма (створена за допомогою бібліотеки Plotly) демонструє, що 52% часу студенти витрачають на розваги, 28% – на навчання, а решту – на спілкування.

Соціальні мережі мають подвійний вплив на освітній процес. Їхнє ефективне використання може суттєво підвищити рівень самонавчання, розширити доступ до ресурсів і стимулювати професійний розвиток. Проте зловживання соціальними мережами може призвести до втрати продуктивності, дезінформації та психологічних проблем.

Застосування бібліотек Python для аналізу цього феномену дає можливість виявити закономірності, створити чіткі візуалізації та отримати корисні інсайти. Надалі дослідження у цьому напрямку може сприяти розробці рекомендацій для студентів і викладачів щодо ефективного використання соціальних мереж у навчанні.

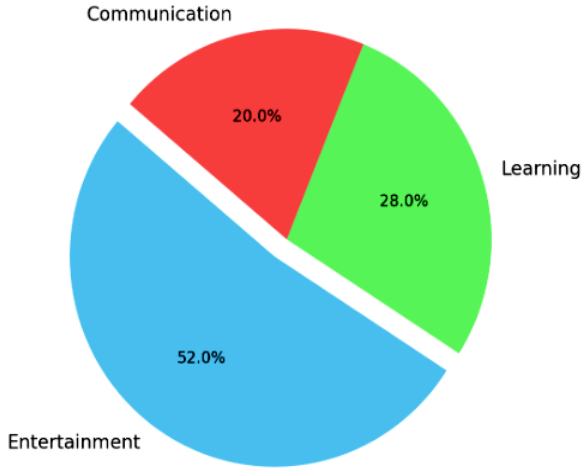


Рисунок 2 – Кругова діаграма

Висновки. Запропонований підхід може бути адаптований для аналізу впливу інших цифрових інструментів на освітній процес, що відкриває нові горизонти для оптимізації навчання у цифрову епоху.

Інформаційні джерела

1. Зацерківна М., & Халіманенко В. (2024). Соціальні мережі як ефективне середовище в освітньому процесі. Цифрова платформа: інформаційні технології в соціокультурній сфері, 7(1), pp. 46–57. URL: https://doi.org/10.31866/2617-796X.7.1.2024.306999

2. Мечус Х., Смотр О., Вовчаста Н., & Рашкевич М. (2022). Дослідження проблематики впровадження технологій гейміфікації у систему освіти. Редколегія, 353 с.

3. Мельничук Я. О., Кравченко С. М. “Аналіз даних та візуалізація за допомогою мови Python”. Житомирський державний технологічний університет. URL: https://eztuir.ztu.edu.ua/bitstream/handle/123456789/7190/54.pdf?sequence=1&isAllowed=y

4. Smotr O., Karabyn O, Malets I., & Golovatyii R. (2024). Research on the feasibility of employing gamification technologies in the training process of IT specialization seekers. CEUR-WS. Proceedings of the IX International Workshop on Professional Retraining and Life-Long Learning using ICT: Person-oriented Approach (3L-Person 2024) co-located with 19th International Conference on ICT in Education, Research, and Industrial Applications (ICTERI 2024). URL: https://ceur-ws.org/Vol-3781/; URL: https://urn:nbn:de:0074-3781-0; URL: https://sci.ldubgd.edu.ua/jspui/handle/123456789/13991

УДК 614.84

"РОЗУМНА ПОЖЕЖНА ЧАСТИНА" – ІННОВАЦІЙНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

Ігор МАЛЕЦЬ
Юрій ГОРНОСТАЙ

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The introduction of a "smart fire department" is an innovative approach to security that integrates modern technologies to improve work efficiency. The main technologies for managing "smart fire departments" are: a system for monitoring the conditions of the working area, a tracking system, a dispatcher interface, an automated lighting control system, etc.*

Keywords: *"Smart fire department", tracking system, IoT solution, air pollution sensor.*

Анотація. *Впровадження "розумної пожежної частини" є інноваційним підходом до забезпечення безпеки, який інтегрує сучасні технології для підвищення ефективності роботи. Основними технологіями для керування "розумними пожежними частинами" є: система для контролю за умовами робочої зони, система трекінгу, інтерфейс диспетчера, автоматизована система керування освітленням тощо.*

Ключові слова: *"розумна пожежна частина", система трекінгу, IoT-рішення, датчик забрудненості повітря.*

У сучасному світі збільшення кількості надзвичайних ситуацій висуває нові виклики до роботи оперативно – рятувальних служб. Ефективність та швидкість їх дій є визначальними факторами для збереження життя людей та мінімізації матеріальних втрат.

Виклики сучасного суспільства показують, що використання автоматизованих, та комп'ютеризованих систем у всіх галузях, в тому числі і в ДСНС, є запорукою зменшення ризику виникнення небезпек. Аналіз існуючих заходів безпеки показує, що використання систем для моніторингу та управління процесами безпеки є вкрай необхідним. Тому й запропоновано впроваджувати концепцію "розумної пожежної частини", яка інтегруватиме сучасні IoT-рішення, автоматизацію та інтелектуальні системи. Встановлено, що впровадження "розумної пожежної частини" дозволить значно покращити ефективність роботи оперативно – рятувальних служб завдяки вико-

ристанню сучасних технологій. Така інтеграція допоможе зменшити час реагування на надзвичайні події.

Основними технологіями, що використовуються є:

1. Системи для контролю за умовами робочої зони, а саме:

– датчик забрудненості повітря (метою використання якого є оперативна оцінка ризиків забруднення та планування дій щодо захисту персоналу);

– датчики моніторингу CO_2 (датчики для контролю рівня вихлопних газів);

– мікрокліматичні сенсори (датчики для контролю температури та вологості в приміщенні, та навколишнього середовища).

2. Система трекінгу (GPS – трекери для моніторингу місцезнаходження пожежних автомобілів та оптимізації їх маршрутів).

3. Інтерфейс диспетчера (інтеграція даних у реальному часі для швидкого прийняття рішень, а також використовується для контролю за освітленням, вентиляцією та іншими автоматизованими системами).

4. Автоматизована система керування робочим, черговим освітленням (інтелектуальна система вмикання/вимикання світла залежно від умов та потреб оперативної роботи).

Дослідження показують, що впровадження розумної пожежної частини має багато переваг, а саме:

1. *Безпека персоналу*. Найважливішою перевагою є підвищення рівня безпеки особового складу.

2. *Швидкість реагування*. Інтегровані системи моніторингу дозволяють оперативно отримувати дані про зміну умов навколишнього середовища, що покращить якість та швидкість реагування.

3. *Ефективність роботи*. Автоматизований аналіз інформації скорочує час на прийняття рішень.

4. *Економічні питання*. Автоматизовані системи вплинуть на економічну складову роботи за рахунок зниження енергоспоживання (завдяки автоматизації) та оптимізація маршрутів зменшить використання палива тощо.

5. *Екологічна безпека*. Контроль за рівнем викидів CO_2 та економія ресурсів сприяють збереженню довкілля.

Висновки. Отже, “розумна пожежна частина” є інноваційним підходом до забезпечення безпеки, який інтегрує сучасні технології для підвищення ефективності роботи та зниження ризиків. Її впровадження сприяє не лише оперативності та надійності оперативно – рятувальних служб, а й покращенню умов праці персоналу та збереженню екологічних ресурсів.

УДК 331.5.07

ЦИФРОВІ РОБОЧІ МІСЦЯ ЯК АЛЬТЕРНАТИВА ТРУДОВІЙ МІГРАЦІЇ

Мудрак ВІТАЛІЙ
Академія праці, соціальних відносин і туризму м. Київ, Україна.

Abstract. *Determined that the general development of technologies contributes to increased mobility of labor resources. Attention is focused on the fact that the digitalization of society's life within the framework of the implementation of the Industry 4:0 concept allows working for companies, including foreign ones, without changing the place of actual residence.*
Keywords: *digitalization, job opportunities, migration.*

Анотація. *Визначено, що загальний розвиток технологій сприяє підвищенню мобільності трудових ресурсів. Акцентовано увагу на те, що цифровізація життя суспільства в рамках реалізації концепції Індустрія 4:0 дозволяє працювати на компанії, у тому числі іноземні, не змінюючи місця фактичного проживання.*
Ключові слова: *цифровізація, робочі місця, міграція.*

Підвищення мобільності капіталу призвело до того, що він почав створювати попит на робочу силу по всьому світові незалежно від країни свого походження, причому не тільки з причин, пов'язаних з нестачею місцевої робочої сили. Використання іноземної робочої сили може мати такі економічні переваги, як рівень кваліфікації працівників, їх більша дисциплінованість, менш високі вимоги щодо рівня заробітної плати тощо [3]. Це явище – трудова міграція – не оминуло і Україну.

Якщо говорити про явище трудової міграції як про переміщення саме робочої сили, а не наслідок вимушеної міграції населення, то найбільшу користь від цього отримує економіка тієї країни, до якої мігрують працівники. *По-перше,* такий працівник привозить унікальний власний досвід, набутий на попередніх місцях роботи, при цьому роботодавцю не потрібно витрачати кошти на навчання нового фахівця. *По-друге,* він заповнює вільне робоче місце на ринку країни, на яке не можуть або не хочуть претендувати місцеві мешканці, адже у розвинутих економіках встановлено низку обмежень, за якими місцеві працівники мають перевагу над іноземною робочою силою, тобто, за нормальних умов така міграція не витісняє місцевих працівників та не призводить до підвищення рівня безробіття. *По-третє,* офіційно оформлений іноземний працівник сплачує податки та користується послугами за місцем свого перебування, чим також робить внесок до розвитку місцевої економіки.

Однак завжди є ризик того, що такий працівник залишиться в країні перебування, влаштувавшись там на постійну роботу та отримавши офіційний дозвіл на постійне проживання, і перевезе туди свою родину, що буде означати остаточну втрату трудової сили для України. Адже, як свідчать результати опитувань, працівники, які виїжджають працювати за кордон вперше, переважно налаштовані повернутися назад із заробленими грошима, але у процесі отримання працівником досвіду роботи у якості трудового мігранта збільшується ймовірність переїзду такого працівника за кордон на постійне проживання [4, с. 8].

Розглядаючи процеси, які відбуваються в Україні, не можна не відзначити, що після початку повномасштабного вторгнення до економічних чинників, котрі спричиняють трудову міграцію, додався фактор війни. Так, за оцінками Інституту демографії та проблем якості життя НАНУ, до початку повномасштабної війни близько 3 млн українців були трудовими мігрантами, а після 24 лютого 2022 року до них додалися ще 6,5 млн. [1].

У довоєнний період не можна було однозначно сказати про те, що міграція справляє негативний вплив на ринок праці України, оскільки за умови її відсутності рівень безробіття був би значно вищим [4, с. 9]. Але зараз ситуація суттєво інша. В той час, коли, за інформацією ресурсу “Work.ua”, загальна пропозиція вакансій на ринку праці у січні 2024 року майже досягла довоєнного рівня (93% до показника лютого 2022 року), попит на ці посади не відповідає довоєнному, причинами чого є як міграція працездатного населення за кордон, так і релокація підприємств, що змінило структуру попиту на робочу силу та призвело до того, що роботодавці стикаються з нестачею кваліфікованих працівників [2].

Крім того, якщо говорити про міграцію та пов’язані з нею проблеми, то не можна обійти стороною питання нелегальної трудової міграції, оскільки такі мігранти піддаються додатковим ризикам, які полягають у частковій або повній втраті прав громадян на території тієї країни, де вони перебувають та працюють неофіційно: неунормовані умови праці, несплата соціальних внесків, відсутність впевненості у власному майбутньому, не кажучи про можливість під час пошуків подібної роботи натрапити на шахраїв та опинитися у рабстві.

Інша ситуація з цифровими робочими місцями: працівник може, перебуваючи на території однієї країни, працювати на роботодавця, зареєстрованого у іншій. Це явище під певним кутом зору навіть можна розглядати не як безпосередньо міграцію робочої сили, а як інвестицію у трудові ресурси з боку іноземних компаній. При цьому економіка тієї країни, у якій перебуває працівник, отримує додаткові кошти, адже такий працівник проживає та користується благами на території своєї країни. У цьому є суттєва відмін-

ність від трудової міграції, коли працівник у будь-якому випадку вимушений витрачати частину зароблених коштів у країні свого перебування, *наприклад*, для задоволення таких базових потреб, як житло або харчування.

Крім того, під час повномасштабної війни частина працівників, які виїхали за кордон (або перемістилися до іншого, більш безпечного, регіону України), можуть продовжувати повноцінно виконувати усі або принаймні частину своїх трудових обов'язків віддалено, якщо побудова робочих процесів не вимагає обов'язкової присутності на робочому місці. Тим більше, частина подібних процесів вже пройшла випробування під час глобальної пандемії COVID-19, тому такі умови роботи не є чимось абсолютно новим ані для працівників, ані для роботодавців.

Більше того, переведення частини робочих місць до категорії цифрових повністю збігається із змінами, викликаними Четвертою промисловою революцією. Концепція Індустрії 4:0 передбачає, що у майбутньому певна частина робочих процесів будуть проводитися із залученням сучасних інформаційних технологій, зокрема, із використанням можливостей глобальної мережі Інтернет [5–7]. І якщо європейські країни останніми роками активно займаються впровадженням цифрових технологій на виробництвах, то в України все це ще попереду. Врахувавши світовий досвід впровадження таких змін, маємо можливість уникнути помилок щодо більш швидкого впровадження технології Індустрії 4:0, сумістивши це з євроінтеграційними процесами, скоротити відставання від розвинених країн світу та посісти достойне місце у глобалізованому світі.

Висновки. Отже слід пам'ятати про те, що збереження трудового потенціалу є важливим за будь-яких умов. Працюючи віддалено, працівник має можливість перебувати у комфортних для нього умовах, у знайомому оточенні. А працюючи за кордоном як трудовий мігрант, працівник перебуває у незвичному для нього середовищі, часто – у іншому культурному просторі. Подібні фактори за своєю сукупністю навряд чи можуть позитивно вплинути на психоемоційний стан людини, що, своєю чергою, не сприятиме підвищенню працездатності працівника.

Інформаційні джерела

1. Брак робочої сили може стати бар'єром на шляху повоєнного відродження. Укрінформ. URL: https://www.ukrinform.ua/rubric-society/3838779-brak-robocoi-sili-moze-stati-barerom-na-slahu-povoennogo-vidrodzenna-ekspert.html (дата звернення: 25.04.2024).

2. Відновлення ринку праці в Україні в умовах війни: регіональні аспекти. Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/doslidzhennya/sotsialna-polityka/vidnovlennya-rynku-pratsi-v-ukrayini-v-umovakh-viyny-rehionalni (дата звернення: 25.04.2024).

3. Козар В. В. Вплив глобалізації світового ринку праці на ефективність використання трудового потенціалу України. International Journal of Innovative Technologies in Economy. 2018. № 2 (14). – С. 51–59.

4. Малиновська О. А. Трудова міграція: соціальні наслідки та шляхи реагування. Київ: НІСД, 2011. 40 с.

5. Петько С. М. Безконтактні послуги мережі 5G в цифровій економіці Республіки Корея. Наукові перспективи. 2024. № 9 (51). – С. 731–743. URL: https://doi.org/10.52058/2708-7530-2024-9(51)-731-743

6. Петько С. М. Технології індустрії 4:0 у цифровій парадигмі розвитку глобальної економіки. Економічний вісник Національного технічного університету України "Київський політехнічний інститут" : зб. наук. пр. / Нац. техніч. ун-т України "КПІ ім. Ігоря Сікорського"; [редкол.: Кравченко М. О. (голов. ред.) та ін.]. – Київ : Вид. дім "Гельветика", 2022. Вип. 24. – С. 51–62. URL: https://doi.org/ 10.32782/2307-5651.24.2022.8

7. Сигида Л. О. Індустрія 4.0 та її вплив на країни світу. Економіка та суспільство. 2018. № 17. – С. 58–64.

УДК005.8:004

УПРАВЛІННЯ РИЗИКАМИ В ІТ-ПРОЄКТАХ

Любов ПЕРЕТЯТКО
Ігор СТЕЦІВ
Кафедра права та менеджменту у сфері цивільного захисту Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *Risk management is primarily the identification of potential threats that may affect a project. This is done using techniques such as brainstorming, interviews with experts, and analysis of data from previous projects.*
Keywords: *projects, risks, management, technology.*

Анотація.*Управління ризиками в першу чергу є визначення потенційних загроз, які можуть вплинути на проєкт. Для цього використовуються такі техніки, як мозковий штурм, інтерв'ю з експертами та аналіз даних з попередніх проєктів.*
Ключові слова: *проєкти, ризики,управління, технології.*

У сфері ІТ-проєктів управління ризиками відіграє ключову роль у забезпеченні успішного досягнення цілей проєкту. Зі зростаючою складністю та залежністю від технологій ІТ-проєкти стикаються з численними ризиками, які можуть вплинути на терміни виконання, бюджети та загальні цілі. Ефективні практики управління ризиками дозволяють керівникам проєктів проактивно ідентифікувати, оцінювати та зменшувати ризики, мінімізуючи їхній негативний вплив. У цій статті ми розглянемо важливість управління ризиками в ІТ-проєктах і ключові етапи цього процесу.

Ідентифікація ризиків. Першим етапом управління ризиками є визначення потенційних загроз, які можуть вплинути на проєкт. Це передбачає всебічний аналіз таких факторів, як вимоги проєкту, технологічні залежності, очікування зацікавлених сторін і зовнішні впливи. Для цього використовуються такі техніки, як мозковий штурм, інтерв'ю з експертами та аналіз даних з попередніх проєктів.

Оцінка ризиків. Після визначення ризиків наступним етапом є оцінка їхнього потенційного впливу та ймовірності виникнення. Це включає аналіз наслідків кожного ризику та оцінку ймовірності його реалізації. Для цього можна використовувати матрицю ризиків або систему оцінювання, які дозволяють категоризувати ризики за їхньою важливістю та визначати пріоритети для подальших дій. Основна мета – зосередитися на найкритичніших ризиках, які потребують негайної уваги.

Розробка стратегій пом'якшення ризиків

Після оцінки ризиків важливо розробити стратегії їхнього пом'якшення для мінімізації впливу або ймовірності виникнення. Це може включати впровадження запобіжних заходів, створення планів дій у надзвичайних ситуаціях або альтернативних підходів. Співпраця з зацікавленими сторонами, експертами та членами команди допомагає розробити ефективні стратегії, адаптовані до конкретного контексту проєкту.

Моніторинг і контроль ризиків

Управління ризиками є безперервним процесом протягом усього життєвого циклу проєкту. Необхідно встановити надійний механізм моніторингу та контролю для відстеження визначених ризиків і заходів з їхнього зменшення. Регулярні огляди статусу проєкту, звіти про прогрес і оновлення реєстру ризиків дають змогу керівникам проєктів оперативно реагувати на зміни у ризиковому середовищі та вживати заходів, якщо ризики посилюються або з'являються нові.

Комунікація та залучення зацікавлених сторін

Ефективна комунікація є ключовою в управлінні ризиками. Керівники проєктів мають інформувати зацікавлені сторони про визначені ризики, стратегії їхнього пом'якшення та потенційний вплив на проєкт. Залучення зацікавлених сторін до обговорення ризиків і прийняття рішень сприяє створенню атмосфери спільної відповідальності та співпраці в управлінні ризиками.

Основні етапи управління ризиками

Методологія PMBOK пропонує чотири основні етапи управління ризиками:

Ідентифікація ризиків

Цей етап включає визначення всіх потенційних загроз, що можуть вплинути на досягнення цілей проєкту. В IT-проєктах найчастіше зустрічаються технічні ризики, такі як проблеми інтеграції, несумісність технологій

чи низька продуктивність. Однак більш складними є ризики, пов'язані з людським фактором: недостатня підтримка керівництва, опір користувачів або партнерів, відсутність належного фінансування.

Аналіз ризиків

Завданням цього етапу є оцінка імовірності настання ризиків і їх впливу на проєкт. Пріоритет надається найбільш критичним ризикам, адже спроба боротися з усіма загрозами одночасно є економічно неефективною.

Планування заходів

Для кожного ключового ризику розробляються стратегії реагування:

Transfer – передача відповідальності за ризик стороннім сторонам, *наприклад*, через страхування чи контракти.

Accept – прийняття ризику без додаткових дій, якщо його наслідки мінімальні.

Mitigate – зниження впливу ризику шляхом застосування проактивних заходів і підготовки альтернативних планів.

Моніторинг та контроль

Постійне оновлення плану управління ризиками та оперативне реагування на нові загрози є невід'ємною частиною успішного виконання проєкту.

Практичні методи управління ризиками

Серед поширених інструментів прогнозування ризиків у світовій практиці використовуються:

Buffer time. Додавання резервного часу до планових строків виконання завдань.

PERT-аналіз. Розрахунок середньої тривалості виконання завдань із врахуванням оптимістичних, песимістичних та очікуваних строків.

Метод Монте-Карло. Статистичне моделювання для прогнозування ризиків і визначення ймовірності їх впливу.

Управління ризиками є невід'ємною частиною управління IT-проєктами, що дає змогу командам проєктів проактивно реагувати на потенційні виклики та забезпечувати успішне виконання завдань. Завдяки ідентифікації, оцінці та зменшенню ризиків керівники проєктів можуть мінімізувати негативний вплив непередбачуваних подій, підвищити продуктивність проєкту та збільшити довіру зацікавлених сторін.

Важливо формувати культуру обізнаності щодо ризиків у межах команди та організації, де управління ризиками стає невід'ємною частиною планування й виконання проєктів.

Висновки. Управління ризиками – це не про усунення всіх ризиків, це стратегічне керування, що дозволяє досягти цілей проєкту з мінімальним рівнем невизначеності. Систематичний та проактивний підхід до управління ризиками дає змогу командам IT-проєктів впевнено долати виклики та досягати успішних результатів.

Інформаційні джерела

1. A Guide to the Project Management Body of Knowledge. (PMBOK Guide) – Fifth edition. Project Management Institute, 2013.

2. Bentley C. PRINCE2: A Practical Handbook – Third Edition. London, UK: Routledge, 322. 2020.

3. The Risk Management Process in Project Management by Brenna Schwartz Feb 26, 2021.

4. Industry in Ukraine. Inforgraphic Atlas. (2017). TOP LEAD with IDC Information Technology.

УДК 330

ВИКОРИСТАННЯ ЦИФРОВИХ ІНСТРУМЕНТІВ ТА ТЕХНОЛОГІЙ ДЛЯ УПРАВЛІННЯ КОМАНДОЮ

Любов ПЕРЕТЯТКО
Павліна ДУБИНЕЦЬКА
Кафедра права та менеджменту у сфері цивільного захисту Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The use of digital technologies and tools for team management helps to increase productivity and reduces the risk of information loss.*

Keywords: *digital technologies, team, digital tools, communication.*

Анотація. *Використання цифрових технологій та інструментів для управління командою сприяє підвищенню продуктивності та зменшує ризик втрати інформації.*

Ключові слова: *цифрові технології, команда, цифрові інструменти, комунікація.*

Роль цифрових технологій у сучасному управлінні командами

У сучасному світі цифровізація стала невід'ємною частиною управління командами. Використання цифрових інструментів дозволяє оптимізувати робочі процеси, підвищувати ефективність командної роботи та забезпечувати швидкий обмін інформацією. Це особливо актуально в умовах глобалізації, коли команди часто працюють дистанційно.

Популярні цифрові інструменти:

– Планувальники завдань та проєктів:

– Інструменти, такі як Trello, Asana та Jira, дозволяють керівникам команд відстежувати виконання завдань, розподіляти обов'язки та планувати терміни. Вони надають можливість візуалізувати робочі процеси через канбан-дошки або календарі, що спрощує координацію роботи.

Інструменти для комунікації:

– Slack, Microsoft Teams та Zoom є ключовими платформами для обміну повідомленнями, проведення відеоконференцій та спільної роботи. Завдяки цим інструментам команди можуть підтримувати високий рівень комунікації навіть у віддаленому форматі.

Облачні платформи для зберігання даних:

– Google Workspace, Dropbox та Microsoft 365 дозволяють зберігати, обмінюватися та одночасно редагувати документи, презентації чи таблиці. Це сприяє підвищенню продуктивності та зменшує ризик втрати інформації.

Переваги цифрових технологій

Ефективність:

– Автоматизація рутинних процесів, таких як управління графіками чи створення звітів, дозволяє співробітникам зосередитися на більш стратегічних завданнях.

Дистанційна робота:

– Використання цифрових технологій забезпечує можливість працювати з будь-якого місця, що є важливим в умовах сучасних викликів, таких як пандемія чи війна.

Прозорість:

– Інструменти відстеження прогресу дають змогу всім членам команди бачити статус завдань, що зменшує кількість непорозумінь.

Виклики цифровізації

Навчання співробітників:

Не всі працівники володіють достатніми навичками для роботи з новими технологіями. Це вимагає проведення тренінгів і навчання, які можуть зайняти час та ресурси.

Кібербезпека:

– Захист корпоративних даних є важливим аспектом, особливо при роботі через віддалені мережі. Організація повинна забезпечити надійні системи захисту від кібератак.

Баланс технологій і людського фактора:

– Надмірна залежність від цифрових інструментів може призводити до втрати особистого контакту в команді. Це може впливати на емоційний стан співробітників та рівень довіри.

Інтеграція цифрових інструментів у командну роботу

– Впровадження цифрових технологій має бути поступовим і враховувати специфіку команди.

Важливо. Організувати тренінги для співробітників, аби вони розуміли, як працювати з новими інструментами. Залучати співробітників до процесу вибору технологій, щоб вони відповідали їхнім реальним потре-

бам. Створити чіткі політики використання технологій для уникнення помилок чи непорозумінь.

Реальні приклади успішного використання цифрових технологій

Microsoft Teams у великих корпораціях:

– Забезпечує централізовану платформу для обміну інформацією, відеоконференцій та спільної роботи. Це особливо актуально для розподілених команд.

Trello для стартапів:

– Інструмент, що дозволяє налаштовувати гнучкі робочі процеси та візуально відображати прогрес завдань.

Рекомендації для ефективного використання цифрових інструментів:

– Регулярно аналізувати ефективність обраних інструментів і за потреби їх змінювати.

– Використовувати аналітику та звіти для оцінки результативності команди.

– Інтегрувати гейміфікацію для підвищення мотивації співробітників.

Висновки. Використання цифрових інструментів та технологій стає ключовим фактором успішного управління командами у сучасному бізнес-середовищі. Вони дозволяють не лише оптимізувати процеси, а й створити гнучке та адаптивне робоче середовище. Попри виклики, такі інструменти допомагають досягати високої продуктивності та підтримувати злагоджену роботу команди навіть у кризових умовах.

Інформаційні джерела

1. Бабак Н. В. Цифрові інструменти для управління командою: сучасні виклики та можливості. Київ: Національний університет імені Тараса Шевченка, 2023.

2. Хомяк І. П. Ефективне використання технологій у командному менеджменті. Журнал “Управління персоналом”, №2, 2022. – С. 45–53.

3. Компаньйола О. В. Використання платформ для віддаленої роботи в сучасному бізнесі. Видавництво “Розумні рішення”, Львів, 2021.

4. Mc Kinsey & Company. How Digital Tools Boost Team Collaboration and Productivity. URL: www.mckinsey.com

5. HubSpot Blog. Top Tools for Remote Team Management in 2024. URL: www.hubspot.com

Напрям 16

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

УДК 004.8:004.056

SAFE INTEGRATION OF THE LANGUAGE MODEL OF ARTIFICIAL INTELLIGENCE IN AN INTERACTIVE SUPPORT SCENARIO TRAINING CLASSES IN REAL TIME. VULNERABILITIES AND RISKS IN USING APPLYING AI MODELS

Petro VENHERSKYI
Sviatoslav BOLISHCHUK
Maksym OSKIRKO
Dmytro PELESHKO

Faculty of Applied Mathematics and Informatics Ivan Franko National University of Lviv, Lviv, Ukraine.

Анотація. *Це дослідження представляє розробку веб-додатку, спрямованого на покращення взаємодії студент-викладач у навчальному процесі шляхом включення штучного інтелекту (ШІ). Програма полегшує спілкування, створення тестів, збір відгуків і підтримку в режимі реального часу, підвищуючи ефективність і результативність онлайн-навчальних середовищ. Дослідження підкреслює вплив систем штучного інтелекту на взаємодію студента та викладача, зосереджуючись на таких факторах, як комунікація, підтримка та присутність, а також визначає такі теми, як відповідальність, зв'язок, свобода волі та спостереження. Щоб усунути вразливості, були проаналізовані такі ризики, як отруєння моделі, і розглянуто методи пом'якшення, включаючи навчання з підкріпленням і диференціальну конфіденційність, для безпечної інтеграції ШІ. Модель OpenAI GPT було вибрано для надання функцій, керованих штучним інтелектом, забезпечуючи надійне та безпечне впровадження.*

Основною метою було розробити веб-додаток, який би покращив взаємодію студентів і викладачів у навчальному процесі шляхом створення додаткового шляху спілкування та співпраці між ними, який би використовував впровадження системи штучного інтелекту (AI) у цього процесу, вивчення можливості використання таких систем і технологій у навчальному процесі, а також вразливості та ризики такого використання.

Ключові слова: *ШІ в освіті, веб-додаток, рольова автентифікація, взаємодія студент-викладач, уразливості, OpenAI GPT, тести самооцінки, підтримка в реальному часі.*

Abstract. *This study presents the development of a web application aimed at enhancing student-teacher interactions in the educational process by incorporating artificial intelligence (AI). The application facilitates communication, test generation,*

feedback collection, and real-time support, improving the efficiency and effectiveness of online learning environments. The research highlights the influence of AI systems on student-lecturer interactions, focusing on factors like communication, support, and presence, and identifies themes such as responsibility, connection, agency, and surveillance. To address vulnerabilities, risks like model poisoning were analyzed, and mitigation methods, including reinforcement learning and differential privacy, were considered for safe AI integration. OpenAI's GPT model was selected to provide AI-driven functionalities, ensuring reliable and secure implementation.

The main objective was to develop a web application that would improve the interaction of students and teachers in the educational process by creating an additional path of communication and cooperation between them, which would take advantage of the introduction of an artificial intelligence (AI) system into this process, study the possibility of using such systems and technologies in the educational process, as well as the vulnerabilities and risks of such use.

Keywords: *AI in education, web application, role-based authentication, student-teacher interaction, vulnerabilities, OpenAI GPT, self-assessment tests, real-time support.*

1. Analysis of the application of AI technologies in the educational process

Despite the promising potential of Artificial Intelligence (AI), the impact of AI systems on student-lecturer interactions remains uncertain. In online learning, student-lecturer interactions have a significant impact on student satisfaction and learning outcomes. Therefore, determining how students and lecturers perceive the impact of AI systems on their interactions is essential to identifying any gaps or issues that prevent AI systems from realizing their potential and compromise the security of these interactions.

The study analyzed research on how AI systems affect student-lecturer interactions in online learning and identified it's factors of interaction such as communication, support, and presence, which allowed us to identify six main themes that describe the impact of AI: quantity and quality, responsibility, just-in-time support, agency, connection, and surveillance. After that, the boundaries beyond which AI systems are perceived as harmful and potential solutions were identified [1].

2. Vulnerabilities and risks when using AI models

Analyzing current risks and vulnerabilities when using AI models is a necessary step to create a safe and ethical environment for their implementation. Given the rapid pace of technological development, it is important not only to understand current risks, but also to anticipate possible future challenges in order to effectively minimize their impact on society.

Certain types of attacks on artificial intelligence systems have already been formalized and some mitigation options have been proposed. For example, model poisoning attacks, the task of which is to harm the system by manipulating training data to degrade the accuracy or directionality of work. An example of mitigation is the implementation of new standards, such as reinforcement learning with human feedback or differential privacy [2].

The use of the OpenAI API and the GPT model was chosen for integration into the system, as they are already established and implement certain aspects of safe AI implementation.

3. Safe integration of the language model of artificial intelligence in an interactive support scenario training classes in real time

During the development, a web application was created to encapsulate the capabilities of communication during classes, creation or generation of tests for student self-assessment, use of AI for improved analysis of educational materials, and a feedback system based on a survey on the quality of teaching.

A data flow diagram (fig. 1) of a system that shows the movement of data from one location to another, indicating the processing, storage, and exchange of data between different elements of the system or process.

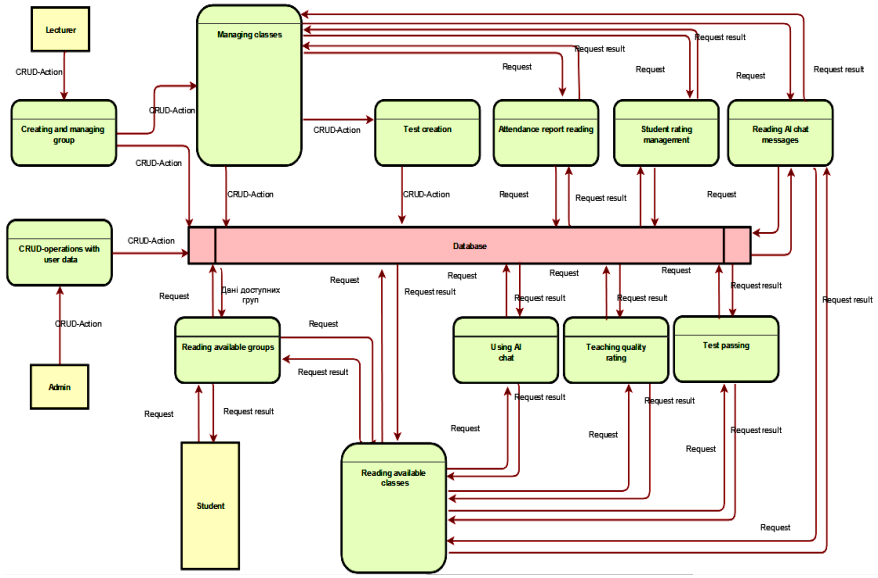


Figure 1 – Data flow diagram of the web-application

The basis of the system is the use of a role-based authentication model. A user can have one of three roles: “Administrator”, “Teacher” or “Student”.

The main work of the administrator is to review requests for registration of new users and manage user accounts, that is, this role gives him access to CRUD functionality over other users.

Management of groups and classes was delegated to the “Teacher” role. He can start a new class, schedule a class, and view details of past classes, namely

attendance and anonymous chat message history. When creating a new class, he has to provide text materials for AI. When planning a class, he also can add questions for self-control. It is also possible to use AI to generate questions on the given material (fig. 2). During the class, the teacher sees the anonymous chat of the group. Separately, this role has the ability to view statistics of grades left by students who attended the class.

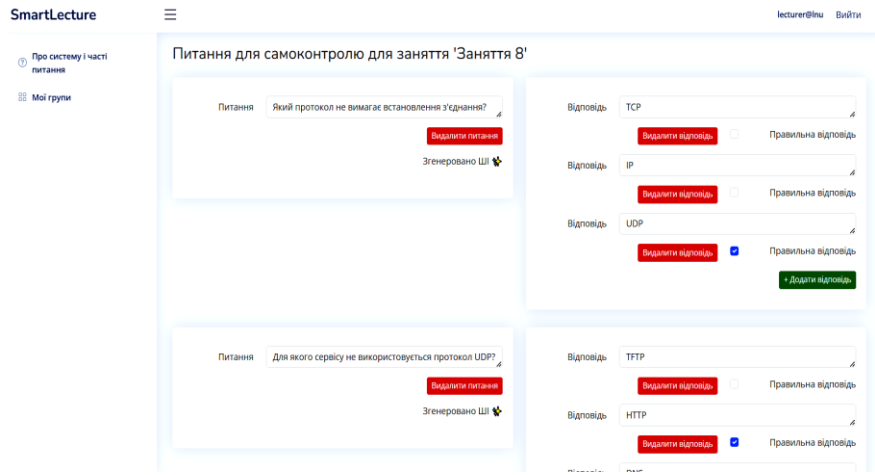


Figure 2 – AI test generation

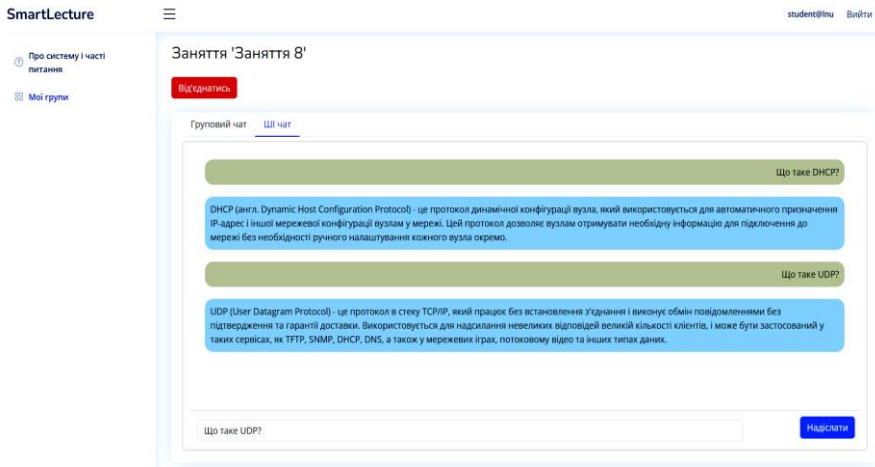


Figure 3 – The use of AI-chat

The “Student” role has access to view the groups to which he belongs, view details of classes that took place in this group, namely the history of anonymous chat messages and AI chat messages, and also has the ability to connect to an active class. During an active class, he can write messages to the anonymous chat or ask questions about the material in the AI chat (fig. 3). It is also possible to leave feedback about the class in the form of a rating on a five-point scale and take a self-control test after its completion.

Information sources

1. The impact of artificial intelligence on learner–instructor interaction in online learning. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8545464/

2. NIST Trustworthy and Responsible AI NIST AI 100-2e2023 Adversarial Machine Learning A Taxonomy and Terminology of Attacks and Mitigations. URL: https://doi.org/10.6028/NIST.AI.100-2e2023

УДК 004.056

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ І ЗАСОБІВ КІБЕРБЕЗПЕКИ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ УКРАЇНИ

Вадим ДУБИНА

Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна.

Abstract. *The article examines the main cyber threats to higher education institutions (HEIs) in Ukraine, including phishing, DDoS attacks, and ransomware. Modern methods of protecting information resources are analyzed, including antivirus software, intrusion detection systems (IDS/IPS), and the use of VPN. Key problems are outlined, including insufficient training of personnel, outdated security systems, and the lack of a unified incident response strategy. Promising areas for improving cybersecurity in HEIs are proposed: implementation of monitoring systems using machine learning, multi-level authentication, regular staff training, and development of rapid threat response strategies.*

Keywords: *cybersecurity, higher education institutions, phishing, DDoS attacks, ransomware, threat monitoring, machine learning, multi-level authentication, response strategy.*

Анотація*. У статті досліджено основні кіберзагрози для закладів вищої освіти (ЗВО) України, серед яких фішинг, DDoS-атаки та програми-вимагачі. Проаналізовано сучасні методи захисту інформаційних ресурсів, включаючи антивірусне про-*

грамне забезпечення, системи виявлення вторгнень (IDS/IPS) та використання VPN. Окреслено ключові проблеми, зокрема недостатню підготовку кадрів, застарілі системи безпеки та відсутність єдиної стратегії реагування на інциденти. Запропоновано перспективні напрями вдосконалення кібербезпеки у ЗВО: впровадження систем моніторингу з використанням машинного навчання, багаторівневої аутентифікації, регулярне навчання персоналу та розробка стратегій швидкого реагування на загрози.

Ключові слова: *кібербезпека, заклади вищої освіти, фішинг, DDoS-атаки, програми-вимагачі, моніторинг загроз, машинне навчання, багаторівнева аутентифікація, стратегія реагування.*

У сучасних умовах високих темпів розвитку інформаційних технологій і зростаючої загрози кіберзлочинності, заклади вищої освіти України є привабливими мішенями для кіберзлочинців. Університети обробляють величезні обсяги конфіденційної та важливої інформації, включаючи особисті дані студентів, наукові розробки та дослідження, що робить їх уразливими до різноманітних типів кібернападів. Тому питання забезпечення належного рівня кібербезпеки є критично важливим для підтримки безпечного освітнього середовища.

Огляд основних загроз

Одним із перших етапів дослідження було детальне вивчення типових кіберзагроз, з якими стикаються університети в Україні. За результатами аналізу, основними видами атак є:

– *Фішинг* – використання підроблених електронних листів для отримання доступу до облікових записів студентів, викладачів та адміністрації.

– *DDoS-атаки* – спроби навантажити сервери університетів, що може призвести до тимчасового знеструмлення електронних ресурсів або порушення навчального процесу.

– *Ransomware* – програмне забезпечення, яке блокує доступ до даних і вимагає викупу за їх відновлення, що є особливо небезпечним для наукових розробок та досліджень.

Аналіз існуючих засобів захисту

Друге завдання дослідження полягало у вивченні вже існуючих методів та інструментів кіберзахисту, що застосовуються в університетах України. Серед найбільш популярних рішень були:

– *Антивірусні програми* – базові інструменти захисту від шкідливих програм, але з обмеженою здатністю протистояти складним кібератакам.

– *Системи виявлення і запобігання вторгненням (IDS/IPS)* – спеціалізовані платформи для моніторингу трафіку та виявлення аномалій, що можуть вказувати на можливі атаки.

Фаєрволи та VPN – застосовуються для фільтрації небажаних з'єднань та забезпечення безпечного доступу до внутрішніх мереж університетів.

Виявилось, що більшість існуючих рішень є фрагментарними і не забезпечують достатнього рівня інтегрованого захисту від нових типів кіберзагроз. Крім того, значна частина університетів не має достатнього фінансування для впровадження новітніх технологій кібербезпеки, що обмежує ефективність існуючих засобів захисту.

Проблеми та виклики

Однією з основних проблем є недостатній рівень підготовки кадрів, відповідальних за кібербезпеку в університетах. Багато закладів не мають спеціалізованих команд для боротьби з кіберзагрозами, що ускладнює ефективне реагування на інциденти безпеки. Крім того, багато університетів не мають єдиної стратегії з кібербезпеки, що також негативно впливає на рівень їх захищеності.

Також варто зазначити, що багато українських університетів застаріли у своєму підході до захисту інформаційних ресурсів. Старі системи безпеки не здатні протистояти новим та складним типам атак, таким як гібридні атаки, комбіновані з соціальною інженерією.

Перспективи розвитку та вдосконалення

У контексті цих проблем, важливим напрямом для вдосконалення системи кібербезпеки в університетах є впровадження інтелектуальних систем моніторингу та прогнозування кіберзагроз, які можуть проактивно виявляти та реагувати на потенційні атаки. Такі системи повинні використовувати методи машинного навчання для аналізу аномальних патернів та своєчасного виявлення нових загроз. Також важливо впроваджувати багаторівневу аутентифікацію для доступу до чутливої інформації, а також інтегрувати механізми швидкого реагування на інциденти безпеки.

Висновки. Загалом, для досягнення високого рівня кібербезпеки в закладах вищої освіти України необхідно здійснювати комплексний підхід, який включає не лише технічні засоби захисту, але й постійну освіту та підготовку персоналу, а також розробку чітких стратегій безпеки.

Інформаційні джерела

1. Про основні засади забезпечення кібербезпеки України [Закон України]: № 2163-VIII від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Державна служба спеціального захисту зв'язку та захисту 1нформаці [державні сайти України]. URL: https://cip.gov.ua/ua.

УДК 37.091.33

ДОПОВНЕНА ТА ВІРТУАЛЬНА РЕАЛЬНІСТЬ У НАВЧАЛЬНОМУ ПРОЦЕСІ ПОЛІЦЕЙСЬКИХ

Роман МУДРОВСЬКИЙ
Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article examines the use of augmented reality (AR) and virtual reality (VR) in police training. The advantages of these technologies are highlighted, in particular the possibility of safely simulating complex situations, personalizing training, and analyzing cadets' actions. The challenges of implementation, including high cost and technical limitations, are outlined, and the prospects for their integration into the training process are determined.*

Keywords: *augmented reality, virtual reality, professional training, police, intelligent systems, tactical skills, artificial intelligence, laser shooting range, educational technologies.*

Анотація. *У статті розглянуто використання доповненої (AR) та віртуальної реальності (VR) у підготовці поліцейських. Висвітлено переваги цих технологій, зокрема можливість безпечного моделювання складних ситуацій, персоналізації навчання та аналізу дій курсантів. Окреслено виклики впровадження, включаючи високу вартість і технічні обмеження, та визначено перспективи їх інтеграції в навчальний процес.*

Ключові слова: *доповнена реальність, віртуальна реальність, професійна підготовка, поліцейські, інтелектуальні системи, тактичні навички, штучний інтелект, лазерний тир, навчальні технології.*

Доповнена (AR) та віртуальна реальність (VR) відкривають нові горизонти у професійній підготовці поліцейських, забезпечуючи сучасний підхід до навчання з акцентом на інтерактивність і безпеку. Завдяки цим технологіям можна моделювати реальні сценарії, які складно або навіть небезпечно відтворювати в умовах традиційного навчального процесу. Це дозволяє правоохоронцям отримувати цінний досвід у контрольованому середовищі, яке забезпечує максимально можливу реалістичність.

Одна з найбільших переваг використання AR і VR полягає у можливості безпечно відпрацьовувати дії в ризикованих ситуаціях. *Наприклад*, курсанти можуть тренуватися в умовах віртуальних перестрілок, масових заворушень або порятунку заручників без ризику для життя. Такі сценарії допомагають не лише розвивати практичні навички, але й формувати психологічну стійкість до стресових умов. Реалістичність VR забезпечується повним зануренням у симульоване середовище з використанням звукових, візуальних і, у деяких випадках, тактильних ефектів.

Доповнена реальність, у свою чергу, накладає віртуальні елементи на реальний світ, створюючи можливості для тренувань у реальному середовищі з додатковою інформацією. *Наприклад*, AR-окуляри можуть показувати інструкції або вказівки під час патрулювання, що дозволяє курсантам отримувати підтримку в реальному часі.

Особливу цінність ці технології мають у розвитку комунікативних та тактичних навичок. За допомогою віртуальних симуляцій курсанти можуть опрацьовувати переговори з правопорушниками, вирішення конфліктів або взаємодію з цивільними в кризових умовах. Це важливий елемент підготовки, оскільки реальні ситуації часто вимагають не лише фізичної, але й психологічної готовності до дій.

Ще однією перевагою є можливість аналізу дій учасників навчання. Системи VR фіксують кожен рух і рішення, що дозволяє детально розбирати помилки та успішні дії. Такий підхід не лише покращує якість навчання, але й сприяє підвищенню впевненості курсантів у власних силах.

Навчальні системи, базовані на штучному інтелекті (AI), також знайшли своє застосування у тактико-спеціальній підготовці поліцейських. Ці системи можуть аналізувати поведінку та реакції поліцейських у симульованих сценаріях, ідентифікувати слабкі місця та рекомендувати покращення. Вони також можуть генерувати персоналізовані навчальні програми, враховуючи індивідуальні потреби та здібності кожного поліцейського. Враховуючи усе вищезазначене, можна розглядати практичні заняття з використанням інтерактивного мультимедійного лазерного тиру (ІМЛТ) як особливий тип навчання. Під час цих занять курсанти отримують міждисциплінарні знання та навички щодо реагування на злочини та правопорушення, застосування поліцейських заходів. Цей підхід ґрунтується на комплексному методі навчання, надаючи можливість виділити основні елементи освіти та встановити взаємозв'язки між навчальними дисциплінами. Є чимало переваг застосування такої технології і насамперед це безпека при проведенні стрільб: Лазерні тири забезпечують високий рівень безпеки порівняно з традиційними стрільбищами. Відсутність реальних набоїв дозволяє уникнути можливих нещасних випадків та травм під час навчання [1].

Втім, впровадження AR і VR у навчальний процес супроводжується низкою викликів. Найсуттєвішим з них є висока вартість обладнання та програмного забезпечення, а також потреба у створенні специфічного контенту, що відповідає реаліям роботи поліцейських. Крім того, не всі навчальні заклади мають достатньо технічних можливостей для впровадження цих інновацій.

Іншою проблемою є адаптація курсантів до роботи з VR-технологіями. У деяких людей використання VR-гарнітури може викликати дискомфорт, зокрема вестибулярні порушення чи зорове перенапруження. Також важливо інтегрувати AR і VR як доповнення до традиційних методів підготовки, щоб забезпечити комплексний підхід до навчання.

Висновки. Попри ці виклики, потенціал AR і VR у навчанні поліцейських важко переоцінити. Ці технології дозволяють створити середовище, у якому курсанти можуть тренуватися ефективніше, безпечніше та з більшим рівнем залученості. Вони сприяють формуванню висококваліфікованих правоохоронців, які здатні діяти професійно навіть у найскладніших умовах. У майбутньому інтеграція доповненої та віртуальної реальності стане важливим кроком до модернізації системи підготовки поліцейських.

Інформаційні джерела

1. Boiko O. I., Melnyk A. M. Prospects for the use of modern interactive technologies in the process of training police officers for activities under martial law. Analytical and Comparative Jurisprudence. 2024, № 3, pp. 297–302. URL: https://doi.org/10.24144/2788-6018.2024.03.50 (дата звернення: 19.11.2024).

УДК 004.6

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ПРОЗОРОСТІ У НАУКОВИХ РЕПОЗИТОРІЯХ УНІВЕРСИТЕТІВ

Павло ГАРАНЬ
Роман ГОЛОВАТИЙ
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *A blockchain-based system is proposed to enhance the security and transparency of the university repository for scientific publications. Blockchain technology ensures data integrity, prevents unauthorized modifications, and increases trust in the storage process of scientific materials. The use of the Spring Boot framework enables the development of a scalable system that simplifies the management and access to publications.*

Keywords: *blockchain, scientific publications, university repository, data transparency, data security, Spring Boot, security, publication management, decentralized system, data verification.*

Анотація. *Запропоновано систему на основі блокчейну для захисту та підвищення прозорості університетського репозиторію наукових публікацій. Технологія блокчейн забезпечує цілісність даних, виключає можливість несанкціонованого редагування та підвищує довіру до процесу зберігання наукових матеріалів. Використання фреймворку Spring Boot дозволяє побудувати масштабовану систему, яка спрощує управління публікаціями та доступ до них.*

Ключові слова: *блокчейн, наукові публікації, університетський репозиторій, прозорість даних, захист даних, Spring Boot, безпека, управління публікаціями, децентралізована система, верифікація даних.*

Сучасна система університетських репозиторіїв наукових публікацій часто стикається з проблемами, пов'язаними з безпекою, прозорістю та довірою до даних. Несанкціоноване редагування інформації, відсутність механізмів перевірки достовірності публікацій та обмежений доступ до них негативно впливають на репутацію установи та ефективність наукових досліджень. У цьому контексті актуальним є впровадження технологій, які забезпечують захист даних, прозорість і довіру до наукового контенту. Однією з таких технологій є блокчейн – децентралізована система зберігання даних, яка гарантує незмінність інформації та доступність для перевірки.

Ця робота пропонує вирішення вказаних проблем через розробку системи університетського репозиторію на основі блокчейну із використанням фреймворку Spring Boot, що дозволяє створити ефективну, масштабовану та безпечну платформу для зберігання та управління науковими публікаціями.

Для вирішення проблеми захисту та підвищення прозорості університетського репозиторію наукових публікацій пропонується інтеграція блокчейн-технології. Основна перевага блокчейну полягає у децентралізованому підході до зберігання даних, що забезпечує їх незмінність та доступність для перевірки. Усі записи в блокчейні є захищеними криптографічними методами, що виключає можливість несанкціонованого редагування.

З точки зору наукової обґрунтованості, блокчейн відповідає ключовим вимогам до зберігання наукової інформації (рис. 1).

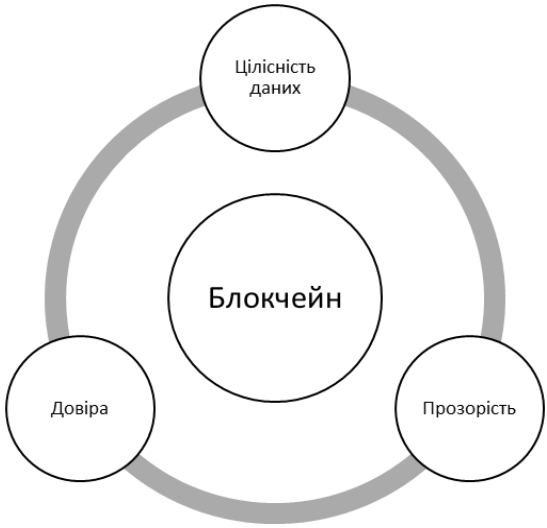


Рисунок 1 – Графічне відображення ключових вимог блокчейну

У даному контексті цілісність публікації, означає, що публікація отримує унікальний ідентифікатор, який гарантує незмінність і точність даних. Щодо прозорості – усі транзакції записуються у відкритий реєстр, доступний для перевірки без посередників. Верифікація даних за допомогою консенсусу виключає підробки, що грунтує рівень довіри між користувачами системи до опублікованих матеріалів.

Для реалізації проєкту обрано фреймворк Spring Boot через його здатність швидко створювати масштабовані веб-додатки, інтеграцію з базами даних та підтримку сучасних архітектурних рішень, таких як REST API. Завдяки Spring Boot забезпечується модульність і зручність розробки, що дозволяє легко реалізувати необхідний функціонал репозиторію. Об'єднання блокчейн-технології та Spring Boot створює основу для побудови системи, яка не лише вирішує проблему безпеки та прозорості, але й відповідає сучасним вимогам до розробки програмного забезпечення.

Розробка системи університетського репозиторію наукових публікацій на основі блокчейн-технології складається з кількох етапів, які представлені на рис. 2.

Рис. 2 – Етапи розробка системи університетського репозиторію наукових публікацій на основі блокчейн-технології

Даний алгоритм забезпечує систематичний підхід до розробки, де кожен етап сприяє досягненню кінцевої мети – створення безпечного, прозорого та зручного репозиторію наукових публікацій.

Запропонована система університетського репозиторію наукових публікацій на основі блокчейн-технології вирішує ключові проблеми сучасних репозиторіїв, такі як відсутність довіри до даних, ризики несанкціонованих змін і обмежена прозорість. Завдяки використанню блокчейну забезпечується цілісність інформації, а також можливість перевірки кожного запису без посередників. Інтеграція фреймворку Spring Boot дозволяє побудувати мас-

штабовану та ефективну систему, яка забезпечує зручність роботи користувачів, гнучкість у розробці нових функцій і надійну обробку запитів. Розроблений алгоритм охоплює всі необхідні етапи створення системи, включаючи проєктування, розробку, тестування та впровадження.

Висновки. Результати даного дослідження демонструють, що поєднання блокчейн-технологій і сучасних засобів розробки програмного забезпечення створює нові можливості для підвищення прозорості та безпеки в управлінні науковими публікаціями. Запропонована система має потенціал для впровадження в університетських установах, сприяючи розвитку науки та полегшуючи доступ до знань.

Інформаційні джерела

1. Зачко О. Б., Головатий Р. Р. Мультиагентна модель управління безпекою при плануванні проектів створення об'єктів з масовим перебуванням людей. Стратегічне управління, управління портфелями, програмами та проектами. 2017. № 2 (1224). – С. 46–51.

2. Смотр О. О., Рашкевич М., Головатий Р., Мечус Х. Використання інструментарію інформаційних технологій для підвищення мотивації студента до навчання у форматі змішаної освіти. Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : Збірник наукових праць. Випуск 6. / За ред. М. С. Коваля, Н. Г. Ничкало. – Львів : ЛДУ БЖД, 2021. – С. 214–217.

3. Борзов Ю., Головатий Р., Магеровський Я. Особливості застосування комп'ютерного моделювання для покращення навчального процесу. Інформаційні технології розвитку змісту освіти. – 2019. – С. 80–81.

УДК 004.056.5:005.8

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ: СУЧАСНІ МОЖЛИВОСТІ ТА ВИКЛИКИ

Олександр ЛЕВКО
Роман ГОЛОВАТИЙ
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The thesis explores the role of information technologies in modern education and their impact on accessibility, flexibility, and quality of learning. It highlights the advantages of implementing technologies such as online courses, interactive resources, 3D modeling, and virtual reality. Issues like cybersecurity, teacher qualification, and maintaining human interaction in the educational process are also addressed. The conclusion emphasizes the need to balance technological innovations with traditional approaches to learning.*

Keywords: *education, information technologies, digitalization, virtual reality, interactive tools, cybersecurity, pedagogy, innovations.*

Анотація. *У роботі розглянуто роль інформаційних технологій у сучасній освіті, їх вплив на доступність, гнучкість та якість навчання. Окреслено переваги впровадження технологій, як-от використання онлайн-курсів, інтерактивних ресурсів, 3D-моделювання та віртуальної реальності. Водночас піднято питання кібербезпеки, кваліфікації педагогів та збереження людського контакту в освітньому процесі. Зроблено висновок про необхідність балансу між технологічними інноваціями та традиційними підходами до навчання.*

Ключові слова: *освіта, інформаційні технології, цифровізація, віртуальна реальність, інтерактивні інструменти, кібербезпека, педагогіка, інновації.*

Сучасний світ неможливо уявити без інформаційних технологій. Вони проникають у всі сфери життя, зокрема й освіту, роблячи її динамічнішою, доступнішою та цікавішою. Технології не просто змінюють те, як ми навчаємося, але й те, як ми розуміємо сам процес навчання. Вони відкривають нові горизонти, і освітня сфера стрімко адаптується до цих змін.

Використання технологій в освіті має багато переваг. По-перше, вони роблять знання доступними для кожного. Онлайн-курси, інтерактивні підручники, дистанційні заняття – усе це дозволяє навчатись незалежно від місця проживання чи соціального статусу. Учень із сільської школи може мати доступ до тих самих навчальних матеріалів, що й студент провідного університету. Це величезний крок у подоланні освітньої нерівності.

По-друге, технології роблять навчання гнучким. Зараз студент може самостійно визначати свій ритм і стиль навчання. *Наприклад*, якщо він краще засвоює інформацію візуально, інтерактивні ресурси, як-от відеоуроки (медіа) чи симуляції, стануть ідеальним інструментом. Це дозволяє будувати індивідуальні траєкторії навчання, які враховують особливості кожного учня.

Звісно, є і технології, які надають ще ширші можливості, як-от 3D-рушії, такі як Unreal Engine, Unity. Вони застосовуються при створенні освітніх симуляцій і віртуальних середовищ. *Наприклад*, у медицині такі платформи допомагають майбутнім лікарям тренувати практичні навички, а в інженерії – моделювати складні проекти. Хоча ці інструменти дуже спеціалізовані, їхній потенціал для розвитку прикладних навичок досить вражаючий. Проте найголовнішою цінністю інформаційних технологій є, звичайно, їх гнучкість. Їх можна застосовувати в будь-якій сфері. *Наприклад*, історія може бути усвідомлена за допомогою яскраво анотованих карт; математика – це вже не лише цифри, а й ігрові програми; а мови краще вивчаються за допомогою програмного забезпечення на телефонах, яке може зв'язуватися з носіями мови. Вони також дозволяють вчителям швидко реагувати, які потім можуть зрозуміти, де знаходяться їхні учні, і скорегувати своє навчання, щоб краще допомогти їм у будь-якій ситуації.

Освіта майбутнього немислима без технологій. Це не тільки розширює наші можливості, але й робить навчання справді цікавим, доступним і сучасним. Водночас важливо пам'ятати, що технології – це лише інструмент.

Найважливішим завжди є процес передачі знань і взаємодія вчителя та учня. Використання технологій у навчанні вимагає від викладачів нового підходу. Роль учителя змінюється: він вже не є єдиним джерелом знань, а виступає наставником, який спрямовує студента у світі інформації. Це створює додаткові вимоги до кваліфікації педагогів, які повинні освоювати нові цифрові інструменти, постійно оновлювати свої навички та вміти працювати у багатофункціональному середовищі.

Не варто забувати й про виклики, які виникають із впровадженням ІТ у навчання. Технології можуть захоплювати, але вони не здатні повністю замінити людський контакт, який залишається важливою складовою навчального процесу. Окрім того, розвиток цифрової освіти потребує значних інвестицій у захист персональних даних. Кібербезпека стає важливим завданням, адже навчальні платформи зберігають чутливу інформацію про студентів і викладачів.

У підсумку, інформаційні технології докорінно змінюють освіту, але водночас вимагають обережності у впровадженні. Головне – зберегти баланс між технологічними інноваціями (рис. 1) та людяністю, адже освіта має на меті не лише передати знання, але й виховати гармонійно розвинену особистість.

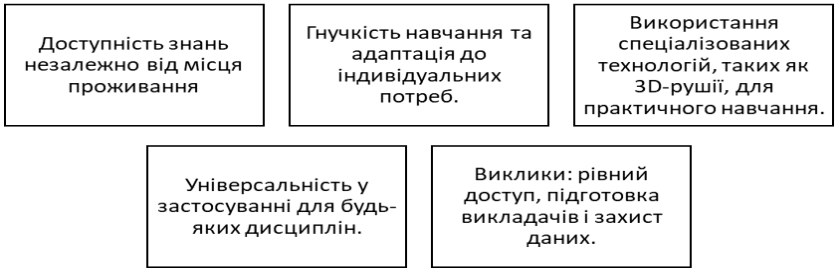


Рисунок 1 – Ключові аспекти впливу технологій на освіту

Інформаційно-комунікаційні технології (ІКТ) справді змінюють освіту в усьому світі; забезпечення безпрецедентного доступу до інформації, знань, а також умінь – практичних навичок. Водночас слід підкреслити, що цей інструмент ефективний у процесі навчання лише тоді, коли цифрова інновація вміло інтегрована з людським виміром.

Висновки. Проблеми цифрового розриву, підготовки вчителів і захисту даних – це те, що робить доступ до якісної освіти абсолютно рівним або конкурентоспроможним для всіх. Освіта виходить за рамки простого когнітивного аспекту та служить для розвитку креативності та критичного мислення людей, щоб стати життєздатними членами світу, що швидко змінюється. Це важливий баланс, який необхідно підтримувати між технічним прогресом і основними цінностями гуманістичної освіти.

Інформаційні джерела

1. Борзов Ю., Головатий Р., Магеровський Я. Особливості застосування комп'ютерного моделювання для покращення навчального процесу. Інформаційні технології розвитку змісту освіти. – 2019. – С. 80–81.

1. Зачко О. Б., Головатий Р. Р. Мультиагентна модель управління безпекою при плануванні проектів створення об'єктів з масовим перебуванням людей. Стратегічне управління, управління портфелями, програмами та проектами. 2017. № 2 (1224). – С. 46–51.

3. Смотр О. О., Рашкевич М., Головатий Р., Мечус Х. Використання інструментарію інформаційних технологій для підвищення мотивації студента до навчання у форматі змішаної освіти. Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : Збірник наукових праць. Випуск 6. / За ред. М. С. Коваля, Н. Г. Ничкало. – Львів : ЛДУ БЖД, 2021. – С. 214–217.

УДК 004.7:373.3+004.9:681.3

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ РУШІЯ UNITY ДЛЯ СТВОРЕННЯ ІГРОВИХ ВІЗУАЛІЗАЦІЙ ТА ЇХНЬОГО ВПЛИВУ НА ЕФЕКТИВНІСТЬ НАВЧАННЯ

Назар БУРАК
Віталій ЯКОВЧУК
Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The paper examines the capabilities of the Unity engine in creating game visualizations that enhance the perception and assimilation of educational content and analyzes their impact on the efficiency of the learning process.*

Keywords: *Unity, game visualizations, educational technologies, learning process, learning efficiency.*

Анотація. *У роботі розглядаються можливості рушія Unity у створенні ігрових візуалізацій, що сприяють кращому сприйняттю та засвоєнню навчального матеріалу, а також аналізується їхній вплив на ефективність освітнього процесу.*

Ключові слова: *Unity, ігрові візуалізації, освітні технології, навчальний процес, ефективність навчання.*

Сучасна освіта дедалі частіше звертається до інтерактивних технологій, які дозволяють залучати здобувачів освіти до активного навчання. У цьому контексті використання ігрових візуалізацій, створених за допомогою рушія Unity, стає одним із найперспективніших напрямів. Unity забезпечує розро-

бникам широкий спектр інструментів для створення реалістичних симуляцій, інтерактивних моделей і віртуальних середовищ, які сприяють глибшому засвоєнню матеріалу. Окрім того інтеграція ігрових механік у навчальні процеси не лише підвищує інтерес до навчання, але й сприяє розвитку критичного мислення, аналітичних навичок та творчості. Це особливо важливо в епоху швидкого технологічного прогресу, коли необхідність адаптивного та ефективного навчання стає критичною для підготовки людей в різних галузях освіти.

Unity є одним із найбільш популярних рушіїв у світі завдяки своїй доступності, універсальності та потужності. Для освітніх установ це означає можливість створення високоякісних навчальних продуктів навіть із обмеженим бюджетом та ресурсами. Безкоштовна ліцензія для навчальних закладів та велика кількість доступних навчальних матеріалів полегшують впровадження цієї технології у навчальний процес.

Крім того, Unity дозволяє створювати продукти, які працюють на різних платформах, включаючи ПК, мобільні пристрої, а також віртуальну та доповнену реальність. Це відкриває нові горизонти для інтерактивного навчання, дозволяючи студентам і викладачам працювати в умовах, максимально наближених до реальних. Ігрові візуалізації, створені за допомогою Unity, дозволяють перетворити складні теоретичні поняття на доступні для розуміння моделі. *Наприклад*, у фізиці чи біології складні явища можуть бути представлені у вигляді інтерактивних симуляцій, що сприяє кращому засвоєнню матеріалу через практичний досвід. Такі методи навчання відповідають принципам сучасної педагогіки, що підкреслюють важливість візуалізації та інтерактивності.

Окрім цього, використання ігрових візуалізацій сприяє підвищенню мотивації студентів. Гейміфікація освітнього процесу робить його більш привабливим і цікавим, що позитивно впливає на рівень залученості та досягнень студентів. Unity, зокрема, надає всі необхідні інструменти для створення таких рішень із високим рівнем деталізації та інтерактивності.

Ігрові рішення, створені на базі Unity, дозволяють враховувати індивідуальні потреби кожного студента. Інтерактивні сценарії можуть адаптуватися до рівня знань користувача, пропонуючи складніші завдання у разі успіху або спрощуючи їх при необхідності. Такий підхід забезпечує ефективніше використання часу й ресурсів як для студентів, так і для викладачів.

Крім того, даний рушій підтримує інтеграцію з технологіями штучного інтелекту, що дає змогу автоматично оцінювати прогрес і адаптувати контент у реальному часі. Це особливо корисно для індивідуального навчання або роботи в умовах великих груп студентів.

Використання Unity у створенні навчальних ігор має значний потенціал для майбутнього розвитку. Технологічні інновації, такі як доповнена та вір-

туальна реальність, дають можливість створювати ще більш реалістичні й захопливі освітні середовища. Це відкриває перспективи для застосування таких продуктів у професійній підготовці, *наприклад*, для тренування медичних працівників чи інженерів у віртуальному середовищі (рис. 1).

Рисунок 1 – Використання рушія Unity для створення VR технологій у навчанні

Постійне оновлення Unity та розширення його функціоналу дозволяє розробникам адаптувати свої продукти до нових викликів і потреб. Інтеграція з іншими технологіями, такими як IoT чи хмарні обчислення, може ще більше підвищити ефективність та зручність навчальних платформ, створених на цьому рушії.

Висновки. Використання рушія Unity відкриває широкі можливості для створення ігор безпекового спрямування, таких як симуляції надзвичайних ситуацій, тренування рятувальників чи навчання з безпеки праці. Такі ігри дозволяють моделювати складні сценарії в контрольованому середовищі, сприяючи формуванню практичних навичок і підвищенню рівня готовності до реальних викликів. Завдяки інтерактивним візуалізаціям та гейміфікації навчання стає ефективнішим, що є важливим кроком у впровадженні сучасних технологій у сферу безпеки.

Інформаційні джерела

1. Можливості ігрових рушіїв у освіті. EDU Technology Blog. URL: https://edutechblog.com/

2. Unity Asset Store як інструмент для швидкої розробки навчальних ігор. Unity Asset Store Blog. URL: https://assetstore.unity.com/blog

УДК 378.1:004.738.5 + 37.091.33

ІНТЕГРАЦІЯ SMART-СИСТЕМ В ОСВІТНЄ СЕРЕДОВИЩЕ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

***Віталій ДЗЕНЬ*[1]**
***Юрій БОРЗОВ*[1]**
***Діана ДЗЕНЬ*[2]**

[1]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.
[2]Національний університет "Львівська політехніка", м. Львів, Україна.

Abstract. *The article analyses the process of integrating smart systems into higher education, their impact on the quality of the educational process, and the main benefits and challenges of implementation. Examples of successful application of smart technologies in various educational environments are discussed.*

Keywords. *Smart systems, adaptive learning, digital transformation, innovative technologies, education automation.*

Анотація. *У статті проаналізовано процес інтеграції smart-систем у вищу освіту, їхній вплив на якість навчального процесу, а також основні переваги та виклики впровадження. Розглянуто приклади успішного використання smart-технологій у різних освітніх середовищах.*

Ключові слова. *Smart-системи, адаптивне навчання, цифрова трансформація, інноваційні технології, автоматизація освіти.*

Модернізація освітнього середовища у контексті цифрової трансформації передбачає впровадження smart-систем, які базуються на технологіях штучного інтелекту, великих даних та автоматизації. Вони сприяють підвищенню ефективності викладання, індивідуалізації навчання та забезпечують доступність освіти незалежно від географічного розташування.

Smart-системи відкривають нові можливості для вдосконалення освітнього процесу у закладах вищої освіти. Вони базуються на використанні технологій штучного інтелекту, великих даних, автоматизації та інтерактивних платформ. Завдяки таким системам можливе створення адаптивних освітніх траєкторій, які підлаштовуються під потреби кожного студента, забезпечуючи персоналізоване навчання. Крім того, smart-системи дозволяють автоматизувати рутинні адміністративні завдання, такі як оцінювання, складання розкладів, управління навчальними матеріалами. Інтеграція інтерактивних елементів, таких як вікторини, симуляції та гейміфікація, робить навчальний процес цікавим і стимулює студентів до активної участі. Вони також сприяють покращенню комунікації між студентами і викладачами завдяки інтеграції засобів онлайн-зв'язку та спільного доступу до ресурсів.

Одним із прикладів ефективного використання smart-систем є українська платформа "E-school", яка забезпечує безкоштовні електронні журнали та

щоденники для навчальних закладів. Ця платформа значно спрощує управління навчальним процесом, автоматизуючи документообіг і забезпечуючи прозорість навчальних досягнень. Ще одним успішним прикладом є система "Classroom", розроблена в Нагойському університеті, яка дозволяє інтегрувати дистанційне та гібридне навчання. Вона включає можливості для проведення інтерактивних занять, тестування, обміну матеріалами та аналізу успішності студентів. Обидва ці приклади демонструють, як smart-технології можуть трансформувати освітнє середовище, підвищуючи його ефективність і адаптивність до сучасних викликів. Перспективи розвитку Віртуального університету Львівського державного університету безпеки життєдіяльності є важливим напрямом для вдосконалення освітнього процесу та підготовки фахівців у сучасних умовах. Система Moodle відкриває широкі можливості для модернізації навчання, але її подальший розвиток вимагає стратегічного підходу та інноваційних рішень. Запровадження аналітичних інструментів для моніторингу успішності студентів і прогнозування потенційних проблем із навчанням, що дозволить викладачам своєчасно реагувати на труднощі та підвищити ефективність навчання.

Інтеграція smart-систем у заклади вищої освіти сприяє значному покращенню якості навчального процесу. Завдяки використанню адаптивних алгоритмів студенти отримують персоналізовані освітні траєкторії, що враховують їхні індивідуальні потреби, рівень підготовки та стиль навчання. Такий підхід не лише підвищує успішність студентів, але й забезпечує їхню глибшу залученість у процес навчання. Крім того, автоматизація рутинних адміністративних завдань, таких як оцінювання, планування та моніторинг, дозволяє викладачам більше зосереджуватися на методичній роботі та особистій взаємодії зі студентами, що позитивно впливає на якість викладання.

Важливим досягненням smart-систем є підвищення доступності освіти. Можливості дистанційного навчання, які вони пропонують, дозволяють студентам отримувати якісну освіту незалежно від їхнього місця перебування. Це особливо актуально в умовах глобальних викликів, таких як війна, блекаути, пандемія COVID-19, коли більшість закладів освіти перейшли на дистанційне навчання. Інтерактивні платформи, елементи гейміфікації, аналітичні інструменти та технології віртуальної реальності роблять навчальний процес не лише ефективним, але й захопливим для студентів.

Водночас інтеграція smart-систем стикається з низкою викликів. Багато закладів освіти не мають належної технічної інфраструктури та фінансових ресурсів для впровадження інновацій. Виникає необхідність у підготовці викладачів до роботи з новими технологіями, що потребує часу та додаткових ресурсів. Окрему увагу слід приділити захисту персональних даних студентів та викладачів, адже сучасні smart-системи активно оперують великими обсягами інформації, яка потребує належного рівня безпеки.

Загалом, впровадження smart-систем є важливим етапом цифрової трансформації освіти, який дозволяє закладам вищої освіти адаптуватися до

сучасних викликів та потреб суспільства. Ці системи створюють нові можливості для вдосконалення навчального середовища, забезпечують рівний доступ до якісної освіти та сприяють підготовці конкурентоспроможних фахівців, здатних працювати у швидкозмінному цифровому світі.

Висновки. Інтеграція smart-систем у заклади вищої освіти є важливим етапом цифрової трансформації освітнього процесу, яка спрямована на підвищення ефективності навчання, індивідуалізацію освітніх траєкторій, автоматизацію рутинних завдань та створення умов для рівного доступу до якісної освіти. Використання таких систем дозволяє значно розширити можливості освітнього середовища, поєднуючи традиційні методи викладання із сучасними цифровими технологіями.

Інформаційні джерела

1. Kim K. Ubiquitous Learning Supporting System for Future Classroom in Korea. Proc. Soc. for Information Technology and Teacher Education : Int'l Conf., K. McFerrin et al., eds. 2008, Mar. pp. 2648–2657.

2. E-school. e-school. URL: https://e-schools.info.

3. Козлова І. М., Баталічева Н. О. Сучасні тенденції розвитку EDTECH компаній та їх вплив на формування маркетингової стратегії у сфері освітніх технологій. Наукові праці МАУП. Економічні науки. 2023. № 2 (69). – С. 47–53.

4. Рибчук А. В.,. Журба І. Є., Процишин О. Р. Цифрова трансформація глобального освітнього середовища. Вісник Хмельницького національного університету. Економічні науки. 2022. № 1. – С. 262–268.

УДК 004.9:371

ІНФОРМАЦІЙНІ СИСТЕМИ УПРАВЛІННЯ ОСВІТНІМ ПРОЦЕСОМ, АРХІТЕКТУРА ТА ОПТИМІЗАЦІЯ ЗА ДОПОМОГОЮ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

***Дмитро АНДРУХІВ*[1]**
***Євген КОБКО*[2]**
***Олександр ПРИДАТКО*[1]**

[1]Львівський державний університет безпеки життєдіяльності, м. Львів, Україна.
[2]Національна академія внутрішніх справ, м. Київ, Україна.

Abstract. *The article examines the role and capabilities of information systems for managing the educational process in modern educational institutions. The key functions of such systems are identified, in particular, the automation of administrative and educational processes, monitoring of success and interactive interaction between participants in the educational process. Architectural features are described, including the client-server model, cloud technologies and distributed systems, which ensure the reliability, scalability and efficiency of information systems. The emphasis is on the advantages of integrating cloud*

computing for distance learning, as well as on examples of international and domestic platforms. The importance of optimizing information systems for improving the quality of learning in the context of the digital transformation of education is emphasized.

Keywords: *information systems for managing the educational process, client-server architecture, cloud technologies, distance learning, monitoring of success, automation of educational processes, digital transformation.*

Анотація. *У статті розглянуто роль та можливості інформаційних систем управління освітнім процесом у сучасних закладах освіти. Визначено ключові функції таких систем, зокрема автоматизацію адміністративних та навчальних процесів, моніторинг успішності та інтерактивну взаємодію між учасниками навчального процесу. Описано архітектурні особливості, серед яких клієнт-серверна модель, хмарні технології та розподілені системи, які забезпечують надійність, масштабованість та ефективність роботи інформаційних систем. Акцентовано на перевагах інтеграції хмарних обчислень для дистанційного навчання, а також на прикладах міжнародних та вітчизняних платформ. Підкреслено важливість оптимізації інформаційних систем для підвищення якості навчання в умовах цифрової трансформації освіти.*

Ключові слова: *інформаційні системи управління освітою, клієнт-серверна архітектура, хмарні технології, дистанційне навчання, моніторинг успішності, автоматизація освітніх процесів, цифрова трансформація.*

Інформаційні системи управління освітнім процесом є ключовим інструментом для ефективної організації та моніторингу навчання в сучасних закладах освіти. Вони дозволяють автоматизувати низку адміністративних та навчальних процесів, від розкладу занять до оцінювання результатів, що значно спрощує роботу викладачів та адміністрації. Оптимізація цих систем за допомогою комп'ютерних технологій, таких як хмарні обчислення та штучний інтелект, дозволяє підвищити їхню продуктивність, гнучкість і безпеку.

Інформаційна система – це сукупність програмних і апаратних засобів, які збирають, зберігають, обробляють і надають інформацію для підтримки прийняття рішень та управління різними процесами. В контексті освіти, такі системи дозволяють автоматизувати багато задач, від реєстрації здобувачів освіти на курси до обробки результатів екзаменів [1]. До основних функцій належать облік здобувачів освіти, планування навчального процесу, моніторинг відвідуваності та успішності, а також автоматизація процесу оцінювання. Вони дозволяють викладачам та адміністрації відстежувати прогрес здобувачів освіти у режимі реального часу, надавати зворотний зв'язок, створювати навчальні матеріали та завдання, а також забезпечувати інтерактивну взаємодію між учасниками навчального процесу.

Серед найбільш популярних інформаційних систем управління освітнім процесом можна виділити як міжнародні, так і вітчизняні рішення. *Наприклад*, Moodle та Blackboard є широко використовуваними у всьому світі платформами для управління курсами, які підтримують онлайн навчання та комунікацію між здобувачами освіти і викладачами. Google Classroom, популярна платформа від Google, дозволяє створювати курси, задавати завдання та відсте-

жувати прогрес здобувачів освіти. В Україні також є приклади впровадження подібних систем, які враховують національні особливості та потреби в освіті. Успішне використання цих систем дозволяє забезпечити гнучкість, інтерактивність і підвищити якість навчання в умовах цифровізації.

Архітектура інформаційних систем управління освітою (ІСУО) є важливим аспектом для забезпечення ефективного управління навчальними закладами, оптимізації навчальних процесів та покращення взаємодії між учасниками освітнього процесу (рис. 1). Основні компоненти та типи архітектури цих систем є ключовими для їх успішного функціонування.

Рисунок 1 – Архітектура інформаційних систем управління освітою

Стосовно типів архітектури, важливо зазначити, що клієнт-серверна модель є однією з основних. У цій моделі система поділяється на два основних компоненти: клієнт, який виконує запити, та сервер, який обробляє ці запити і надає відповідь. Клієнт-серверна архітектура дозволяє централізовано зберігати дані та ресурси, забезпечуючи їх швидкий доступ, що є особливо важливим для освітніх систем, які потребують масштабованості та надійності. Також варто звернути увагу на використання хмарних технологій в освітніх системах, які забезпечують доступ до ресурсів і даних з будь-якого місця, що особливо актуально для дистанційного навчання [3]. Хмара дозволяє знижувати витрати на інфраструктуру, забезпечує легкість у масштабу-

ванні та інтеграції нових функцій. Не менш важливим типом є розподілені системи, які забезпечують можливість роботи декількох незалежних комп'ютерних систем, що взаємодіють між собою для досягнення спільної мети. У контексті освіти це може бути використано для інтеграції різних освітніх платформ, обміну даними між навчальними закладами та створення складних навчальних середовищ.

У сучасному світі інформаційні системи управління освітою (ІСУО) піддаються постійним змінам і вдосконаленням завдяки впровадженню новітніх комп'ютерних технологій. Оптимізація цих систем не лише підвищує їх ефективність, але й робить освітній процес більш доступним, зручним та індивідуалізованим. Однією з найбільш значущих інновацій є хмарні обчислення. Ця технологія дозволяє зберігати дані та виконувати обробку на віддалених серверах, що значно зменшує витрати на локальну інфраструктуру. Хмарні рішення забезпечують гнучкість у доступі до даних, дозволяючи викладачам та здобувачам отримувати необхідну інформацію з будь-якої точки світу. Наступним кроком у розвитку ІСУО є інтелектуальні аналітичні системи, які дозволяють моніторити результати навчання та прогнозувати успішність здобувачів освіти. За допомогою цих систем навчальні заклади можуть отримувати детальну інформацію про досягнення здобувачів освіти, аналізувати тенденції та надавати рекомендації щодо покращення навчальних процесів. *Наприклад*, система може виявити, які теми викликають труднощі у здобувачів освіти, і пропонувати додаткові ресурси або індивідуальну підтримку. Значний потенціал для оптимізації навчального процесу також має машинне навчання та штучний інтелект.

Ці технології сприяють індивідуалізації навчального процесу, адаптуючи навчальні матеріали відповідно до потреб і стилів навчання кожного здобувача освіти [4]. Завдяки цьому кожен здобувач отримує можливість вчитися у своєму темпі, що покращує загальні результати навчання. Планування навчальних програм також може бути автоматизоване за допомогою спеціалізованих програмних рішень, що аналізують дані про доступність викладачів, аудиторій та здобувачів. Таке автоматизоване планування дозволяє уникнути конфліктів у розкладах і забезпечити оптимальне використання ресурсів навчального закладу. Крім того, ведення електронних журналів є ще однією сферою, де автоматизація приносить значні переваги. Завдяки автоматизованим системам управління даними, викладачі можуть легше відстежувати присутність, оцінки та інші важливі показники, спрощуючи документообіг і підвищуючи точність даних. В результаті впровадження цих технологій спрощується робота викладачів та адміністрації. Вони можуть зосередитися на навчальному процесі та розвитку своїх здобувачів, замість того щоб витрачати час на рутинні адміністративні завдання. Оптимізація інформаційних систем управління освітою за допомогою сучасних комп'ютерних технологій не лише підвищує їх ефективність, але й значно

покращує якість навчання. Хмарні обчислення, інтелектуальні аналітичні системи, машинне навчання та автоматизація рутинних процесів формують новий освітній ландшафт, що відповідає потребам сучасного суспільства. Це дозволяє навчальним закладам бути більш адаптивними, інноваційними та зосередженими на досягненні успіху своїх здобувачів освіти.

Впровадження інформаційних систем управління освітою (ІСУО) має потенціал значно покращити навчальні процеси, проте супроводжується рядом викликів та проблем. Ці виклики можна умовно поділити на технічні, соціальні та питання безпеки.

Одним із найбільших технічних викликів є вартість впровадження нових інформаційних систем. Витрати на ліцензування програмного забезпечення, оновлення обладнання, навчання персоналу та технічну підтримку можуть бути значними, особливо для навчальних закладів з обмеженим бюджетом. Багато університетів не можуть собі дозволити необхідні інвестиції, що призводить до нерівності в доступі до сучасних технологій. Ще однією важливою технічною проблемою є вимоги до інфраструктури. Системи потребують надійної мережевої інфраструктури, яка може включати в себе швидкісні інтернет-з'єднання та відповідне обладнання. У багатьох випадках навчальні заклади мають застарілі системи, які не відповідають сучасним вимогам, що ускладнює впровадження нових рішень [5].

Соціальні аспекти також відіграють важливу роль у впровадженні ІСУО. Рівень цифрової грамотності викладачів та здобувачів може значно варіюватися. Якщо викладачі не мають достатніх знань та навичок для використання нових технологій, їхнє впровадження може бути малоефективним. Крім того, здобувачі, які не мають доступу до технологій або не вміють їх використовувати, можуть відчувати труднощі в навчанні, що підвищує ризик виникнення цифрової нерівності. Адаптація до нових технологій також є важливим аспектом. Як викладачі, так і здобувачі повинні мати можливість швидко пристосуватися до нових платформ і програм. Без належної підтримки та навчання це може призвести до опору змінам, що перешкоджатиме успішному впровадженню систем.

Висновки. Питання безпеки є критично важливими в контексті освітніх інформаційних систем. Захист персональних даних здобувачів повинен бути пріоритетом для навчальних закладів, оскільки вони обробляють чутливу інформацію, включаючи особисті дані та академічні результати. Ненадійні системи можуть бути вразливими до витоків інформації, що загрожує безпеці здобувачів і може призвести до серйозних наслідків. Також кібербезпека в освітніх системах є важливим аспектом. Зловмисники можуть намагатися отримати доступ до систем для крадіжки даних або для використання ресурсів навчальних закладів у зловмисних цілях. Важливо, щоб навчальні заклади впроваджували сучасні технології захисту, такі як шифрування, системи аутентифікації та регулярні перевірки безпеки, щоб запобігти можливим загрозам.

Інформаційні джерела

1. Дубов Д. В., Ожеван О. А., Гнатюк С. Л. Інформаційне суспільство в Україні: глобальні виклики та національні можливості: аналіт. доп. – К.: НІСД. – 2010. – 64 с.
2. Гриценко В. Г. Місце і роль інформаційно-комунікаційних технологій у навчанні упродовж життя. Наука і освіта – №3/CXII, 2013 – Психологія і педагогіка: Тематичний випуск "Традиції та новації сучасної освіти в Україні". – 2013. – С. 53–57.
3. Гриценко В. Г. Використання хмаро орієнтованих засобів ІКТ для підвищення якості освіти. Черкаському національному університету ім. Б. Хмельницького – 95: історія та сучасність: [матеріали Всеукраїнської науково-практичної конференції 26 лютого 2016 року]. – Черкаси, 2016. – С. 50–51.
4. Гриценко В. Г. Організаційно-методичні засади використання хмарних сховищ даних для роботи з навчально-методичними комплексами дисциплін. Вища освіта України №3 (додаток 1) – 2012 р. Тематичний випуск "Педагогіка вищої школи: методологія, теорія, технології". – Т.3. – С. 393–402.
5. Жалдак М. І. Проблеми інформатизації навчального процесу в середніх і вищих навчальних закладах. Комп'ютер в школі та сім'ї – № 3 – 2013 – С. 8–15.

УДК 378.147:004.356.2

ПОТЕНЦІАЛ ЗАСТОСУВАННЯ FDM ДРУКУ В ОСВІТНЬОМУ ПРОЦЕСІ

Семен ОСКЕРКО
Ігор МАЛЕЦЬ

Кафедра інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The possibilities of implementing FDM printing in the educational process to increase student motivation through a system of material incentives and practical training are studied. The methodology of integrating additive technologies into the educational process is considered and the implementation results are analyzed.*

Keywords: *FDM printing, educational process, student motivation, additive technologies.*

Ключові слова: *Досліджено можливості впровадження FDM-друку в освітній процес для підвищення мотивації студентів через систему матеріальних заохочень та практичного навчання. Розглянуто методологію інтеграції адитивних технологій у навчальний процес та проаналізовано результати впровадження.*

Ключові слова: *FDM-друк, освітній процес, мотивація студентів, адитивні технології.*

Сучасний освітній процес вимагає впровадження інноваційних підходів для підвищення ефективності навчання та мотивації студентів. Технологія FDM-друку представляє собою потужний інструмент, який може бути вико-

ристаний для створення унікальної системи заохочень та практичного навчання. Метою дослідження є розробка методології впровадження FDM-друку в освітній процес та аналіз його впливу на якість навчання.

Технологія FDM-друку базується на пошаровому нанесенні розплавленого термопластичного матеріалу. Основними технологічними параметрами є температура екструзії, швидкість друку, висота шару та щільність заповнення. В освітньому середовищі найчастіше використовуються такі матеріали як PLA (полілактид) – безпечний біорозкладний пластик, PETG – міцний матеріал з хорошими механічними властивостями, та TPU – гнучкий матеріал для спеціальних застосувань.

Основним напрямком застосування FDM-друку в освітньому процесі є створення системи матеріальних заохочень. Практика показує, що персоналізовані нагороди, виготовлені за допомогою 3D-друку, суттєво підвищують мотивацію студентів до навчання. Такі нагороди можуть включати іменні статуетки для відмінників, тематичні медалі за досягнення в окремих дисциплінах та спеціальні відзнаки за перемоги в студентських олімпіадах. Важливою перевагою є можливість швидкого створення та модифікації дизайну нагород відповідно до конкретних потреб та досягнень.

Особливу цінність мають функціональні винагороди, які студенти можуть використовувати в повсякденному навчанні. Це можуть бути персоналізовані органайзери, тримачі для канцелярського приладдя, захисні кейси для електронних пристроїв. Такий підхід не лише стимулює навчальну активність, але й демонструє практичне застосування технології FDM-друку.

Важливим аспектом є практичне навчання студентів роботі з FDM-технологіями. Процес навчання починається з вивчення базових принципів роботи обладнання та основ 3D-моделювання. Поступово студенти освоюють налаштування програмного забезпечення для підготовки моделей до друку та вивчають техніку безпеки при роботі з обладнанням. Наступним етапом є освоєння оптимізації параметрів друку та роботи з різними матеріалами.

У процесі навчання студенти опановують навички усунення типових несправностей та здійснення постобробки надрукованих моделей. Особлива увага приділяється розвитку навичок модифікації принтерів та створення складних багатокомпонентних моделей. Студенти вчаться розробляти власні профілі друку та оптимізувати параметри відповідно до конкретних завдань.

Методика впровадження FDM-друку передбачає створення спеціалізованої лабораторії та навчання викладацького складу. Необхідним є формування технічної бази, що включає 3D-принтери початкового рівня з закритим корпусом, станції для постобробки моделей, системи вентиляції та фільтрації повітря, а також комп’ютери з відповідним програмним забезпеченням.

Важливим елементом є розробка методичних матеріалів та формування банку 3D-моделей для практичних занять. Навчально-методичне забезпе-

чення має включати інструкції з техніки безпеки, навчальні посібники з 3D-моделювання та практичні завдання різних рівнів складності. Організація конкурсів та проєктів стимулює творчий підхід студентів до навчання.

Практичне застосування FDM-друку охоплює широкий спектр навчальних дисциплін. У природничих науках технологія використовується для створення молекулярних моделей, анатомічних макетів та геометричних фігур. В інженерних дисциплінах здійснюється прототипування механізмів та створення функціональних моделей. У сфері мистецтва та дизайну технологія застосовується для створення архітектурних макетів та дизайнерських прототипів.

Результати впровадження FDM-друку демонструють значне підвищення успішності студентів та зростання відвідуваності занять. Спостерігається збільшення кількості студентських проєктів та підвищення їхньої якості. Більшість студентів успішно освоюють базові навички роботи з адитивними технологіями, а найбільш зацікавлені досягають високого рівня майстерності.

Важливим результатом є формування у студентів комплексного розуміння технологічного процесу та розвиток практичних навичок. Студенти навчаються не лише користуватися готовими рішеннями, але й розробляти власні проєкти, враховуючи технічні обмеження та оптимізуючи параметри друку для досягнення найкращих результатів.

Подальший розвиток впровадження FDM-друку передбачає створення онлайн-курсів та розширення технологічних можливостей через інтеграцію з сучасними системами автоматизації. Планується розробка спеціалізованих навчальних матеріалів та власних технічних рішень. Особлива увага приділятиметься розвитку міждисциплінарних зв’язків та реалізації комплексних проєктів.

Висновки. Отже, результати проведеного дослідження свідчать про значний потенціал використання FDM-друку для підвищення якості освіти та мотивації студентів. Система матеріальних заохочень у поєднанні з практичним навчанням створює ефективне середовище для розвитку професійних компетенцій. Результати дослідження підтверджують доцільність подальшого розширення використання адитивних технологій у навчальному процесі.

Інформаційні джерела

1. Манжілевський Д. О. Сучасні адитивні технології 3D друку. Особливості практичного застосування [Книга].

2. Морзе Н. Впровадження технології 3D друку в освітньому процесі [Журнал]: Київський університет імені Бориса Грінченка, 2017.

3. Войцеховська О. О. Сучасні технології та засоби 3D-моделювання та 3D-друку у закладах вищої освіти [Журнал]. – Київ : 2022.

4. Олексишен О. В. Серія “Нові рішення в сучасних технологіях” [Книга].

5. Фещук Юрій. Впровадження технології 3-D друку в процес підготовки майбутніх учителів трудового навчання та технологій [Книга]. – 2022.

УДК 004.056:371.4

КІБЕРБЕЗПЕКА ДІТЕЙ ТА МОЛОДІ: ПРОФІЛАКТИКА ТА ОСВІТА

Дмитро ІЛЬЧУК
Навчально-науковий інститут № 4 Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The article explores the importance of integrating cybersecurity into the school curriculum as a key stage in the formation of students' digital literacy. The contribution of popular online platforms, such as Coursera, edX, Udemy, LinkedIn Learning, and FutureLearn, to the development of cybersecurity skills at different levels of training is analyzed. The features, accessibility, interactivity, and certification of the educational programs of each platform are considered. It is found that Coursera and edX are leaders in academic learning, Udemy provides practical content, LinkedIn Learning is oriented towards professionals, and FutureLearn is noted for its accessibility and interactivity for beginners. The need to adapt educational materials in the school environment to constantly changing digital technologies and cyberthreats is emphasized.*

Keywords: *cybersecurity, digital literacy, online platforms, Coursera, edX, Udemy, LinkedIn Learning, FutureLearn, integration into education, school curriculum, educational technologies.*

Анотація*. Стаття досліджує важливість інтеграції кібербезпеки в шкільну програму як ключовий етап формування цифрової грамотності учнів. Аналізується внесок популярних онлайн-платформ, таких як Coursera, edX, Udemy, LinkedIn Learning та FutureLearn, у розвиток навичок з кібербезпеки на різних рівнях підготовки. Розглянуто особливості, доступність, інтерактивність і сертифікацію навчальних програм кожної платформи. Виявлено, що Coursera та edX є лідерами в академічному навчанні, Udemy надає практичний контент, LinkedIn Learning орієнтований на професіоналів, а FutureLearn відзначається доступністю та інтерактивністю для новачків. Підкреслено необхідність адаптації навчальних матеріалів у шкільному середовищі для постійно змінюваних цифрових технологій та кіберзагроз.*

Ключові слова: *кібербезпека, цифрова грамотність, онлайн-платформи, Coursera, edX, Udemy, LinkedIn Learning, FutureLearn, інтеграція в освіту, шкільна програма, навчальні технології.*

Інтеграція кібербезпеки у шкільну програму, особливо у курс інформатики, є важливим кроком для формування цифрової грамотності. У рамках таких програм дітей навчають базовим принципам безпеки: уникненню фішингових пасток, створенню надійних паролів та відповідальному використанню соціальних мереж. У багатьох країнах Європи кібербезпека є обов'язковим елементом шкільного курсу, а Україна лише розвиває цей напрямок, хоча подібні ініціативи вже впроваджуються через пілотні проекти, перевага шкільної освіти полягає в її широкому охопленні, проте адаптація матеріалів до постійних змін у сфері цифрових технологій потребує значних ресурсів.

Існує багато платформ для опанування кібербезпеки, протк у навчальній роботі розписані та поєднані між собою найкращі. Coursera є платформою, що вирізняється співпрацею з провідними університетами та компаніями, такими як IBM, Google і Stanford. Вона пропонує структуру навчання на рівні університетських курсів із можливістю отримання сертифікатів, які визнаються в професійному середовищі. Зокрема, спеціалізація Cybersecurity Fundamentals by IBM охоплює основні аспекти кібербезпеки. Курси на Coursera часто включають теоретичні основи, практичні завдання та перевірку знань, що робить платформу чудовим вибором для тих, хто прагне серйозної підготовки.

edX, як і Coursera, також співпрацює з провідними освітніми установами, такими як MIT і Harvard. Однак головна особливість edX – це його акцент на глибоких технічних аспектах і академічному підході. *Наприклад*, курси кібербезпеки тут зазвичай фокусуються на системах криптографії, аналізі мереж і захисті великих даних. edX також дозволяє отримати професійні сертифікати, а в багатьох випадках кредити для подальшого навчання в університетах, що робить його корисним для студентів.

Udemy займає іншу нішу, орієнтуючись на практичний підхід до навчання. На платформі представлений широкий спектр курсів для будь-якого рівня підготовки – від новачків до професіоналів. *Наприклад*, The Complete Cyber Security Course by Nathan House пропонує покрокове вивчення кібербезпеки з акцентом на реальних сценаріях, таких як захист приватності в Інтернеті. Udemy вигідно вирізняється доступністю за ціною, регулярними знижками на курси, але не пропонує університетських сертифікатів, що може бути мінусом для професійної атестації.

LinkedIn Learning пропонує курси, які орієнтовані на розвиток професійних навичок. Платформа має тісний зв’язок із LinkedIn, що дозволяє автоматично додавати сертифікати про завершення курсу до вашого профілю. Курси, такі як основи мережевої безпеки або етичний хакінг, відзначаються компактністю, що підходить для швидкого навчання. Однак матеріал часто менш глибокий у порівнянні з Coursera чи edX, що може не задовольнити тих, хто шукає детальний технічний аналіз.

FutureLearn має унікальний підхід, зосереджуючись на доступності освіти через інтерактивне навчання. Курси, такі як Introduction to Cyber Security, охоплюють ключові концепції без зайвих технічних складнощів, що робить платформу чудовим вибором для новачків. Важливою особливістю є спільнота студентів, яка заохочує обмін досвідом і колективне вирішення завдань. Однак глибина контенту може бути недостатньою для просунутих спеціалістів.

Якщо порівнювати доступність навчання, то Udemy та FutureLearn є найбільш доступними завдяки низьким цінам і безкоштовним курсам. Coursera та edX, попри вищу вартість, пропонують фінансову допомогу або безкоштовний доступ до матеріалів без сертифікації. LinkedIn Learning стоїть посередині за ціною, але має інтеграцію з професійною мережею LinkedIn. В плані якісного контенту Coursera і edX лідирують завдяки своїм зв'язкам з університетами. Udemy пропонує більш прикладний і практичний підхід, але якість контенту залежить від автора курсу. LinkedIn Learning і FutureLearn більше орієнтовані на початковий та середній рівень підготовки. Інтерактивність також відрізняється: FutureLearn фокусується на спільному навчанні через форуми і групові завдання, тоді як LinkedIn Learning забезпечує короткі відеоуроки без значної взаємодії. Coursera та edX часто пропонують форуми і завдання, які допомагають зануритись у матеріал. Udemy надає перевагу самостійній роботі. Щодо сертифікації, Coursera та edX мають перевагу завдяки сертифікатам від університетів. LinkedIn Learning дозволяє демонструвати сертифікати роботодавцям, а FutureLearn також надає сертифікацію, але її визнання залежить від роботодавця. Udemy має найменшу вагу сертифікатів через неофіційний характер курсів.

Висновки. Кожна платформа має свої переваги. Coursera і edX найкраще підходять для серйозного академічного навчання та кар'єрного зростання. Udemy є чудовим вибором для швидкого освоєння практичних навичок. LinkedIn та Learning добре підходить для професіоналів, які хочуть швидко отримати нові навички, а FutureLearn є оптимальним для новачків завдяки інтерактивному підходу та доступності.

Інформаційні джерела

1. Coursera. URL: https://www.coursera.org/courseraplus/?utm_medium=sem&utm_source=gg&utm_campaign=b2c_emea_coursera-plus_coursera_ftcof_subscription_oct-24_dr_geo-multi-set3_sem_rsa_gads_lg-en&campaignid=21836581620&adgroupid=168083277774&device=c&keyword=coursera&matchtype=e&network=g&devicemodel=&adposition=&creativeid=718590612126&hide_mobile_promo&gad_source=1&gclid=Cj0KCQiA0fu5BhDQARIsAMXUBOKLIB_oOIoOIVv8MFveuedoRwjyfk4p3gRsgj_RMing9wla1mmBiwaAvkcEALw_wcB (дата звернення: 21.11.2024).

2. Огляд онлайн-курсів Udemy 2024 року – чи варто? URL: https://www.websiteplanet.com/uk/blog (дата звернення: 20.11.2024).

3. Освітня платформа Future Learn. URL: https://lvet.edu.ua/index.php/mizhnarodna-diialnist/news-intr-m/2840-zaholovok-osvitnia-platforma-future-learn.html (дата звернення: 19.11.2024).

4. Kaspersky Safe Kids. URL: https://support.kaspersky.com/KPC/1.0/uk-ua/95389.htm (дата звернення: 20.11.2024).

УДК 316.644

ВПЛИВ КІБЕРЗАГРОЗ НА МОРАЛЬНИЙ СТАН НАСЕЛЕННЯ

Василь ЛУЧИК
Вікторія ЖУРАВЕЛЬ
Кафедра протидії кіберзлочинності Харківського національного університету внутрішніх справ, м. Кам'янець-Подільський, Україна.

Abstract. *The impact of cyber threats on the morale of the population in the conditions of modern information warfare is studied. The mechanisms of disinformation dissemination, cyber attacks on critical infrastructure and their psychological effect are considered. Ways to counteract the negative consequences of cyber threats are identified, including information hygiene, development of digital literacy and psychological support of citizens.*

Keywords: *cyber threats, morale, psychological stress, cyberbullying, disinformation, critical infrastructure, hybrid warfare, digital technologies, martial law, social stability.*

Анотація. *Досліджено вплив кіберзагроз на моральний стан населення в умовах сучасної інформаційної війни. Розглянуто механізми поширення дезінформації, кібератак на критичну інфраструктуру та їхній психологічний ефект. Виокремлено способи протидії негативним наслідкам кіберзагроз, включаючи інформаційну гігієну, розвиток цифрової грамотності та психологічну підтримку громадян.*

Ключові слова: *кіберзагрози, моральний стан, психологічний стрес, кібербулінг, дезінформація, критична інфраструктура, гібридна війна, цифрові технології, воєнний стан, соціальна стабільність.*

Кіберзагрози мають не лише технічний і економічний, але й глибокий психологічний та соціальний вплив на моральний стан населення. В умовах глобалізації та активного розвитку цифрових технологій, кібератаки та кіберзлочинність набувають все більшої ваги як фактори, що можуть дестабілізувати суспільство, посилюючи страх, невпевненість та деструктивні настрої серед громадян. Особливо це актуально в умовах воєнного стану, коли кіберзагрози стають важливим елементом гібридної війни [1].

Одним з найбільш очевидних наслідків кіберзагроз є психологічний стрес. Кібератаки на критичні інфраструктури, такі як енергетичні мережі, водопостачання, медичні системи або банки, можуть викликати не лише тимчасові труднощі у функціонуванні цих систем, а й значні емоційні реакції у населення. Втрата доступу до основних сервісів і ресурсів, відсутність електрики чи води, порушення зв'язку може призвести до паніки серед громадян. Люди можуть відчувати себе безпорадними і вразливими, що впливає на їхній моральний стан, посилюючи відчуття небезпеки та невизначеності.

Крім того, кіберзагрози часто супроводжуються інформаційними атаками, такими як пропаганда, поширення фейкових новин і дезінформації.

Особливо у воєнних умовах ці атаки стають частиною психологічної війни. Дезінформація здатна підривати довіру до державних інституцій, створювати атмосферу страху та хаосу. Коли люди стикаються з протиріччями в повідомленнях, суперечливими новинами або цілеспрямованими маніпуляціями, це може викликати почуття безпорадності та тривоги, що ще більше посилює моральний стрес у суспільстві.

Додатково, кібербулінг і онлайн-харасмент, які часто є результатом використання технологій для маніпулювання людьми або організаціями, можуть стати серйозним чинником, що впливає на моральний стан окремих громадян. Постійна атака в інтернеті, загрози, публічні приниження чи кібератаки на особисті акаунти можуть викликати не лише психологічний дискомфорт, але й депресії, тривогу та низьку самооцінку. Це особливо актуально для молоді, яка активно використовує соціальні мережі.

Виділяють вісім типів поведінки, характерних для кібербулінгу:

1. *Перепалка, або флейм* (від англ. Burning-палючий, Гарячий, полум'яний) – обмін короткими гнівними і запальними репліками між двома або більше учасниками з використанням комунікаційних технологій.

2. *Атаки*, постійні виснажливі випади (від англ. harassment-домагання)- в більшості випадків це образливі повідомлення, спрямовані на адресу жертви (*наприклад*, сотні SMS-повідомлень на мобільний телефон).

3. *Дифамація*, дискредитація (застереження) – використання комп'ютерних технологій для поширення чуток, неправдивої інформації. Це можуть бути текстові повідомлення, фотографії або пісні, які зображують жертву в принизливій, а іноді і сексуальній формі.

4. *Підробка* – зловмисники позиціонують себе як жертви, використовуючи паролі для доступу до таких облікових записів, як соціальні мережі, блоги, електронна пошта та миттєві повідомлення і поширюють негативну інформацію.

5. *Обман*, витік конфіденційної інформації та її поширення (going out & ruse) – отримання особистої інформації під час спілкування і відправка її в загальнодоступну область Інтернету або поштою особі, для якої вона не призначена (текстовим шляхом).

6. *Відчуження (вигнання), ізоляція*. Люди, особливо в дитячому віці, схильні усвідомлювати себе або в групі, або поза групою. Бажання бути включеним до групи є мотивацією багатьох вчинків дітей, особливо підлітків. Виключення з групи сприймається як соціальна смерть. Чим більше людина відсторонений від взаємодії, *наприклад*, від ігор, тим гірше він себе почуває, і його самооцінка значно знижується.

7. *Кіберзлочин* – дії з таємного вистежування особи, яка зазнала переслідування або випадково потрапила в зону інтересу, як правило, таємно, анонімно, з метою організації злочинних дій або фізичного насильства, побиття.

8. Хеппіслеппінг (від англійського happyslapping – щасливі ляскання) – відносно новий вид кіберзапугівання, що зародився в англійському метро,

коли 10-річні підлітки, що прогулювалися поруч з Пероном, несподівано заплескали один одному, а інші учасники зняли це на камери мобільних пристроїв. Надалі відео, на якому було зафіксовано власне напад, отримало назву “хепіслеппінг” [2].

Отже, в усіх описаних формах кібербуллінгу можна виділити булерів, жертв і спостерігачів (глядачів, читачів). Інколи в ролі жертви й булера може бути одна людина: *наприклад*, зазнаючи нападок від одних, вона знаходить слабшу за себе жертву і теж нападає на неї, утворюючи ніби ланцюжок передавання агресії.

Ще одним аспектом є вплив кібератак на довіру до цифрових технологій та інтернет-сервісів. Якщо люди втрачають віру в безпеку своїх персональних даних, це може призвести до загального зниження активності в онлайн-просторі. Люди починають уникати використання онлайн-банкінгу, покупок в інтернеті, соціальних мереж, що в свою чергу негативно позначається на їхньому емоційному стані. Вони починають відчувати невпевненість у своїх фінансових операціях, а в окремих випадках і в здатності захистити свою приватність.

Особливо серйозним є вплив кіберзагроз на моральний стан в умовах воєнного конфлікту. У воєнні часи атаки на інформаційні системи державних структур чи стратегічних об’єктів мають не лише військове значення, а й психологічний вплив на громадян. Вони можуть сприяти відчуттю непевності у завтрашньому дні, підривати моральний дух населення, викликати паніку та дезорієнтацію. Це, в свою чергу, може негативно вплинути на готовність населення підтримувати зусилля держави в умовах війни, спричиняти соціальну напругу.

Висновки. Таким чином, кіберзагрози мають комплексний вплив на моральний стан населення, сприяючи посиленню стресу, тривоги та невизначеності. Особливо в умовах воєнного стану цей вплив стає ще більш потужним, оскільки інформаційні атаки та кібератаки можуть мати серйозні наслідки не лише для фізичної безпеки, а й для психологічної стабільності суспільства. Важливо враховувати цей фактор у процесі розробки стратегій кіберзахисту, які повинні включати не тільки технічні заходи, але й психологічну підтримку громадян.

Інформаційні джерела

1. Поняття та зміст кіберзагроз на сучасному етапі | GOAL. GOAL | Глобальна організація союзницького лідерства. URL: https://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi/ (дата звернення: 16.11.2024).

2. Психологічні особливості кібербулінгу як форми віртуальної агресії у підлітків. IRBNMU – Репозитарій Національного медичного університету імені О. О. Богомольця: Головна сторінка. URL: http://ir.librarynmu.com/bitstream/ 123456789/ 2763/1/Психологічні%20особливості%20кібербулінгу.pdf (дата звернення: 16.11.2024).

3. Як захиститися від кібератак – Системний інтегратор ITBIZ. Системний інтегратор ITBIZ. URL: https://itbiz.ua/statti-ta-obzori/yak-zahistitisya-vid-kiberatak/ (дата звернення: 16.11.2024).

УДК 378

СУЧАСНІ ІНТЕРАКТИВНІ МЕТОДИ ЕФЕКТИВНОГО ВИВЧЕННЯ ІНОЗЕМНОЇ МОВИ МОВИ ЗДОБУВАЧАМИ ВИЩОЇ ОСВІТИ ПРОГРАМИ “ПРАВООХОРОННІ ІНФОРМАЦІЙНІ СИСТЕМИ”

Роксолана ЗАПОТІЧНА
Дніпровський гуманітарний університет. м. Львів, Україна.

Abstract. *This article is aimed at investigating interactive tools and methods for effective English language learning among higher education students in the “Law Enforcement Information Systems” program. In the modern world, where information technology and law enforcement aspects are interconnected, language proficiency becomes a crucial skill for students in this specialization.*

Key words: *English language, information technology professionals, interactive teaching methods, language proficiency, foreign language for professional purposes.*

Анотація. *Здійснено аналіз останніх досліджень та публікацій, що стосуються вивчення англійської мови фахівцями з інформаційних технологій. На основі цього аналізу надано рекомендації та підходи, які можуть бути корисними для здобувачів вищої освіти програми “Правоохоронні інформаційні системи”. Розглянуто конкретні інтерактивні інструменти та ресурси, такі як мовні програми, відеоуроки, онлайн-платформи та інші.*

Ключові слова: *англійська мова, фахівці з інформаційних технологій, інтерактивні методи навчання, мовна компетентність, іноземна мова професійного спрямування.*

*Постановка проблеми***.** Здобувачі вищої освіти програми “Правоохоронні інформаційні системи” мають унікальні освітні потреби, оскільки вони одночасно опановують як базові дисципліни, так і спеціалізовані курси, пов’язані з інформаційно-аналітичним забезпеченням правоохоронних органів, проєктуванням та адмініструванням правоохоронних інформаційних систем. По суті, їх освітні потреби охоплюють як технічний, так і юридичний аспекти.

Однією з ключових проблем є необхідність ефективного вивчення англійської мови з урахуванням специфіки їхньої освіти. Здобувачі вищої освіти повинні не лише володіти загальною лексикою та граматикою англійської, але і розуміти та використовувати спеціалізовані терміни та поняття в області інформаційно-технологічного права та правоохоронної діяльності.

Іншою важливою проблемою є недостатній доступ до адекватних навчальних ресурсів та інтерактивних інструментів, спрямованих на підвищення якості вивчення англійської мови з врахуванням їхніх специфічних потреб. Традиційні методи навчання можуть бути недостатньо ефективними, оскільки вони не завжди враховують технічний та юридичний контекст, який є важливим для майбутніх фахівців в області правоохоронних інформаційних систем.

У даній статті ми розглянемо важливість вивчення англійської мови для здобувачів вищої освіти цієї програми та висвітлимо можливі рішення для покращення процесу навчання, зокрема, через використання інтерактивних інструментів та ресурсів, спеціально розроблених з урахуванням їхніх унікальних потреб.

*Аналіз останніх досліджень і публікацій***.** Останні дослідження свідчать про ефективність інтеграції інформаційних технологій в процес вивчення англійської мови серед фахівців у галузі інформаційних технологій. Використання веб-сайтів, мобільних додатків, відеоуроків та інших технологій дозволяє здобувачам вищої совіти отримувати доступ до різноманітних ресурсів та здійснювати активний навчальний процес.

Однією з важливих тенденцій є адаптація навчального змісту до конкретних потреб фахівців у галузі інформаційних технологій. Дослідження вказують на важливість включення технічної термінології та завдань, які відображають реальні сценарії використання англійської мови в цій галузі.

Останнім часом спостерігається зростання попиту на спеціалізовані курси та сертифікати з англійської мови для фахівців інформаційних технологій. Дослідження вказують на те, що такі курси дозволяють здобувачам вищої освіти підвищити свою конкурентоспроможність на ринку праці та ефективніше спілкуватися в міжнародному співробітництві.

Деякі дослідження досліджують вплив соціокультурних чинників на вивчення англійської мови фахівцями інформаційних технологій. Це включає в себе аспекти культурного адаптування та міжкультурної комунікації в контексті міжнародних команд та проектів. Також останні дослідження вказують на важливість систематичної оцінки результатів вивчення англійської мови серед фахівців інформаційних технологій. Така оцінка дозволяє визначити ефективність методів навчання та внести вдосконалення у навчальний процес.

Метою даної статті є дослідження та аналіз інтерактивних інструментів, які можуть бути використані для ефективного вивчення англійської мови здобувачами вищої освіти програми “Правоохоронні інформаційні системи”. Стаття спрямована на вивчення сучасних методів та ресурсів, які сприяють покращенню мовних навичок та академічного успіху в цій спеціалізації. Разом з тим, метою є також висвітлення актуальності та значущості вивчення англійської мови в контексті програми “Правоохоронні інформаційні системи” та підкреслення важливості інтеграції мовної підготовки з професійною підготовкою у цій галузі.

*Виклад основного матеріалу***.** Перш ніж розглядати інтерактивні інструменти для вивчення англійської мови здобувачами вищої освіти, важливо визначити, чому ця мова є настільки важливою для здобувачами вищої освіти програми “Правоохоронні інформаційні системи”.

Англійська мова є міжнародною мовою комунікації, особливо в галузі інформаційних технологій та правоохоронної діяльності. Здобувачі вищої освіти, які спеціалізуються в "Правоохоронні інформаційні системи", повинні мати навички спілкування, читання, та письма на англійській мові, оскільки багато з понять, технологій та законодавчих актів у цій галузі представлені саме англійською мовою.

Інтерактивні інструменти для вивчення англійської мови стали невід'ємною частиною сучасного освітнього процесу. Вони дозволяють здобувачам вищої освіти активно взаємодіяти з мовним матеріалом та розвивати навички на слух і мовлення. До таких інструментів можуть відноситися:

– Мовні програми та додатки: сучасні мобільні додатки та комп'ютерні програми пропонують інтерактивні уроки, тести та вправи, які допомагають вдосконалити граматику, словниковий запас та вимову. Мовні програми та мобільні додатки, такі як Duolingo, Rosetta Stone, або Babbel, надають здобувачам доступ до інтерактивних уроків та вправ для вивчення англійської мови. Вони можуть бути особливо корисні для самостійного навчання та розвитку граматики та словникового запасу.

– Відеоуроки та вебінари: використання відеоуроків та вебінарів на англійській мові допомагає здобувачам вищої освіти покращити навички слухання та розуміння мовлення носіїв мови. Платформи, такі як YouTube, Coursera, або TED Talks, містять велику кількість відкритих відеокурсів та лекцій з різних тем.

– Онлайн-платформи: існує багато спеціалізованих онлайн-платформ, які пропонують курси з вивчення англійської мови, розроблені спеціально для фахівців у галузі правоохоронних інформаційних систем. Спеціалізовані онлайн-платформи, *наприклад*, Khan Academy, Duolingo English Test, або EnglishClub, пропонують курси з вивчення англійської мови, розроблені спеціально для фахівців у галузі інформаційних технологій.

– Рольові ігри та симуляції: використання рольових ігор або симуляційних завдань, де здобувачі вищої освіти грають ролі та вирішують конкретні сценарії, може допомогти розвивати практичні навички та розуміння ситуацій в контексті професійної діяльності.

– Інтерактивні завдання з реальними сценаріями: використання завдань, які базуються на реальних сценаріях та ситуаціях, може допомогти здобувачам розвивати навички, необхідні для їхньої майбутньої професійної діяльності.

Рольові ігри та симуляції є інтерактивними методами навчання, які можуть бути особливо корисними для здобувачів вищої освіти програми "Правоохоронні інформаційні системи". Ці методи дозволяють здобувачам не просто засвоювати теоретичний матеріал, але і застосовувати свої знання та

навички у конкретних сценаріях, що можуть стати реальними в їхній майбутній професійній діяльності:

– Сценарії на основі реальних ситуацій: рольові ігри та симуляції можуть будуватися на основі реальних ситуацій, з якими можуть стикнутися фахівці в галузі інформаційних технологій та правоохоронної діяльності. *Наприклад*, це може бути симуляція кібератаки на інформаційну систему, де здобувачі вищої освіти виконують ролі аналітиків, програмістів і службовців з безпеки.

– Рольова ідентифікація: кожен учасник рольової гри приймає на себе певну роль або професію, пов'язану з галуззю "Правоохоронні інформаційні системи". Це може включати ролі аналітиків, детективів, інженерів, юристів тощо. Ця рольова ідентифікація допомагає здобувачам вищої освіти краще відчути себе частиною реальної робочої команди та виконувати завдання відповідно до своєї ролі.

В цілому, рольові ігри та симуляції можуть забезпечити здобувачам вищої освіти вищої освіти програми "Правоохоронні інформаційні системи" практичні знання та навички, необхідні для подальшого успішного вирішення завдань у своїй професійній діяльності, особливо в галузі інформаційних технологій та правоохоронної сфери.

Використання інтерактивних інструментів для вивчення англійської мови має численні переваги. Вони включають:

– забезпечення активної практики мовлення та слухання;

– підвищення мотивації здобувачів вищої освіти через цікавий та інтерактивний підхід до навчання;

– зручний доступ до навчального матеріалу в будь-який час та з будь-якого місця;

– можливість використовувати різні типи завдань, такі як відео, аудіо, тестування та інше.

Висновки. Інтерактивні методи навчання відіграють ключову роль у розвитку мовних навичок здобувачів вищої освіти в галузі "Правоохоронні інформаційні системи". Вони сприяють активній взаємодії здобувачів вищої освіти з мовним матеріалом і забезпечують більш ефективне вивчення англійської мови. Завдяки інтерактивним методам навчання, здобувачі вищої освіти в програмі "Правоохоронні інформаційні системи" можуть не лише вивчати англійську мову більш ефективно, але й набувати практичних навичок, які будуть корисні в їхній подальшій професійній діяльності.

Інформаційні джерела

1. Yahrif M. (2019). The Implementation of Roleplay Activities to Get Students Speak. Indonesian EFL Journal: Journal of ELT, Linguistics, and Literature, 5(1), pp. 77–92.

2. Kostikova I., Holubnycha L., Shchokina T., Soroka N., Budianska V., Marykivska H. (2019). A role-playing game as a means of effective professional english teaching. Amazonia investiga. Vol. 8. Is. 24, pp. 414–425.

УДК 378.147:373.3:004](4)

ПРОФЕСІЙНА ПІДГОТОВКА ВЧИТЕЛІВ ПОЧАТКОВОЇ ШКОЛИ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА (ЄВРОПЕЙСЬКИЙ ДОСВІД)

Галина КУЧАКОВСЬКА
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна.

Abstract. *The article explores European practices in the professional training of primary school teachers within the context of societal digitalization. The main focus is on the role of digital competencies in teacher training and the practical application of European competency frameworks. The article demonstrates that European educational systems are actively integrating digital technologies into the training of primary school teachers.*
Keywords: *higher education, professional teacher training, digital competence.*

Анотація. *У статті досліджуються європейські практики професійної підготовки вчителів початкової школи в умовах цифровізації суспільства. Основна увага приділяється ролі цифрових компетенцій у підготовці педагогів та практичне застосування європейських рамок компетентностей. У статті показано, що європейські освітні системи активно інтегрують цифрові технології у підготовку вчителів початкової школи.*
Ключові слова: *вища освіта, професійна підготовка вчителів, цифрова компетентність.*

Метою статті є дослідити європейські практики підготовки вчителів, здатних ефективно використовувати цифрові технології у навчально-виховному процесі, і запропонувати рекомендації щодо їх впровадження в національну систему педагогічної освіти. Для досягнення поставленої мети перед авторами стояли завдання: розглянути, як цифрові технології впливають на освіту та змінюють вимоги до професійної підготовки вчителів початкової школи; проаналізувати передові практики та підходи до підготовки вчителів у європейських країнах, які успішно впроваджують цифрові технології у навчальні програми. Подальших досліджень набуває розробка рекомендації для вдосконалення системи професійної підготовки вчителів початкової школи, враховуючи європейський досвід, та адаптації його до національних умов для підвищення якості освіти в умовах цифрового суспільства.

Основні методи

Аналіз та синтез наукової літератури – для узагальнення сучасних підходів і визначення основних напрямів підготовки вчителів до цифровізації в освітніх системах Європи. Аналіз публікацій, досліджень та освітніх стандартів дає можливість виділити актуальні практики та теоретичні основи.

Порівняльний аналіз – для порівняння моделей професійної підготовки вчителів у різних європейських країнах. Це допомагає виявити спільні риси та особливості підходів до формування цифрових компетентностей у педагогів.

Метод кейс-стаді (case study) – для глибокого вивчення конкретних прикладів успішного впровадження цифрових технологій у педагогічну підготовку в деяких європейських країнах. Це дозволяє дослідити окремі практичні кейси, які можуть бути корисними для впровадження в інших країнах.

Системний підхід – для узагальнення результатів дослідження та побудови комплексного бачення підготовки вчителів у цифровому середовищі, враховуючи всі аспекти: навчальні технології, зміст освіти, методичні підходи та компетентності.

***Основний текст*.** Професійна підготовка вчителів початкової школи в країнах Європи в умовах цифровізації суспільства набуває стратегічного значення, оскільки технології глибоко інтегруються в усі сфери життя, включаючи освіту. Європейські країни активно модернізують свої освітні системи, щоб підготувати вчителів до роботи в нових умовах, де цифрові інструменти стають невід'ємною частиною навчального процесу.

Зі статистични даних Євростат [1] у 2021 році в ЄС було 23,2 мільйона учнів початкової освіти. Найбільша кількість учнів початкової освіти у 2021 році серед країн-членів ЄС становила 4,3 мільйона у Франції. Це було помітно більше, ніж у Німеччині, Іспанії та Італії, де було 3,0 мільйона, 2,9 мільйона та 2,7 мільйона відповідно. У 2021 році в ЄС працювало 1,89 мільйона вчителів початкової школи. Ця цифра не включає вчителів у незалежних спеціальних навчальних закладах Франції та середніх школах Словенії. У 2021 році державою-членом ЄС з найбільшою кількістю вчителів початкової школи (в тисячах) була Німеччина (261 000). Це трохи більше, ніж в Італії (249 000), Іспанії (248 000) і Франції (також 248 000, неповний робочий день).

Цифрові технології та штучний інтелект (ШІ) відіграють все більш важливу роль. Це сприяє знаходженню нових шляхів щодо підвищення рівня цифрової компетентності та рівня сформованості інших компетенцій. Так існуючі європейські рамки компетенцій, такі як DigCompEdu (Європейська рамка цифрових компетенцій для освітян) [2] та AI Competency Framework for Teachers (Рамка компетенцій у сфері штучного інтелекту для вчителів) [3], виступають як критично важливі для підготовки вчителів початкових класів. Ці рамки не лише визначають необхідні знання та навички, а й сприяють формуванню нових підходів до навчання. Рамка DigCompEdu [2] складається з 22 компетенції, організовані в шість основних областей, акцентує увагу не лише на технічних аспектах, а й на тому, як цифрові технології можуть використовуватися для покращення та інновацій в освіті. DigCompEdu пропонує інструменти для самооцінки, що дозволяє педагогам визначити рівень своїх цифрових компетенцій та отримати рекомендації щодо подальшого розвитку. AI competency framework for teachers [3], яка визначає знання, навички та цінності, необхідні для вчителів у епоху штучного інтелекту (ШІ). Рамка спрямо-

вана на різні групи, включаючи політиків, постачальників підготовки вчителів, профспілки вчителів, керівників шкіл і самих вчителів.

У більшості європейських країн у процес підготовки вчителів початкової школи інтегруються дисципліни, що стосуються цифрової грамотності. Майбутні педагоги навчаються використовувати інтерактивні платформи, цифрові навчальні ресурси та програми для віддаленого навчання. *Наприклад*, у Чехії вчителі опановують такі інструменти як Moodle та Google Classroom для організації навчального процесу онлайн [4–7].

Європейські країни, зокрема Німеччина, Франція та Швеція, активно розвивають системи підвищення кваліфікації для діючих вчителів [8–10]. Курси цифрової компетентності, що фінансуються державою або у партнерстві з приватними організаціями, дозволяють педагогам адаптуватися до нових викликів та отримувати практичні знання щодо впровадження технологій в освіту. У багатьох європейських країнах набуває популярності концепція змішаного навчання (blended learning), де традиційні методи поєднуються з цифровими технологіями. Це підхід дозволяє вчителям ефективніше працювати з різними групами учнів, адаптуючи навчальний процес під індивідуальні потреби. *Наприклад*, в Естонії активно використовуються хмарні технології для створення персоналізованих навчальних програм.

Узагальнюючи, складаємо порівняльну таблицю основних аспектів, які можна порівняти між різними європейськими країнами, акцентуючи увагу на підходах до підготовки вчителів (табл. 1), де

Країна: назва європейської країни, досвід якої розглядається.

Підхід до цифрової освіти вчителів: основні принципи та особливості підготовки вчителів у кожній країні, які визначають специфіку їхнього навчання та підтримки.

Ключові компетентності: компетенції, які вважаються важливими у підготовці вчителів до роботи в цифровому середовищі.

Методи підготовки: основні методи, які використовуються для навчання цифрових навичок.

Приклади цифрових інструментів: конкретні платформи та програми, які використовуються для цифрового навчання вчителів у кожній країні.

Таблиця 1.

Порівняння підходів різних країн до цифрової підготовки вчителів

Країна	*Підхід до цифрової освіти вчителів*	*Ключові компетентності*	*Методи підготовки*	*Приклади цифрових інструментів*
Німеччина	Високий рівень підтримки з боку держави; акцент на інтеграцію IT-компетенцій	DigCompEdu, критичне мислення, інформаційна безпека	Змішане навчання, практичні курси	Moodle, Microsoft Teams, HPI Schul-Cloud

Франція	Обов'язкова цифрова грамотність для всіх освітян; партнерство з IT-компаніями	Створення мультимедійного контенту, основи AI	Сертифікація, онлайн-курси	Moodle, Eduscol, Google Classroom
Швеція	Системний підхід до розвитку IT-навичок; технологічне забезпечення шкіл	Самоосвіта, робота з інтерактивними платформами	Співпраця з університетами, практичні тренінги	SchoolSoft, Google Workspace
Чехія	Навчання вчителів цифровим інструментам з акцентом на дистанційне навчання	Використання LMS, основи кібербезпеки	Дистанційні курси, воркшопи	Moodle, Google Classroom
Естонія	Держава фінансує розвиток цифрових компетенцій вчителів	Медіаграмотність, критичний підхід до цифрових джерел	Вебінари, практичні сесії	eKool, Stuudium, хмарні технології

Висновки. Отже, у Європі підготовка вчителів зосереджена не лише на їхніх власних знаннях у сфері IT, але й на вмінні формувати у школярів цифрові навички. Вчителі навчаються використовувати технології для розвитку критичного мислення, творчого підходу та цифрової грамотності серед дітей. Професійна підготовка вчителів початкової школи в європейських країнах є багатогранним процесом, спрямованим на забезпечення педагогів необхідними цифровими компетенціями для ефективної роботи в умовах сучасного цифрового суспільства.

Інформаційні джерела

1. European statistics. URL: https://ec.europa.eu/eurostat

2. Punie Y., editor(s), Redecker C. European Framework for the Digital Competence of Educators: DigCompEdu, EUR 28775 EN, Publications Office of the European Union, Luxembourg, 2017. ISBN 978-92-79-73718-3 (print), 978-92-79-73494-6 (pdf). doi:10.2760/178382 (print),10.2760/159770 (online), JRC107466. URL: https://joint-research-centre.ec.europa.eu/digcompedu_en

3. AI competency framework for teachers. URL: https://unesdoc.unesco.org/ark:/48223/pf0000391104/PDF/391104eng.pdf.multi

4. Záhorec, Ján et al. "Inovácie pregraduálnej prípravy učiteľov v zameraní na formovanie ich digitálnych kompetencií." Journal of Technology and Information Education 12 (2021), pp. 80–92. URL: https://doi.org/ 10.5507/JTIE. 2020.013.

5. Javorcik Tomas and Tatiana Havlaskova. "Level and Ways of Educating Future Teachers in the Use of Digital Technologies: Basic Results of a Questionnaire Survey." 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA) (2020), pp. 254–259. URL: https://doi.org/10.1109/ICETA51985.2020. 9379158.

6. Zounek Jiří, Klára Záleská, Libor Juhaňák. “Výuka s využitím ICT v mezinárodní perspektivě: na cestě k moderní pedagogice.” (2020). URL: https:// lifelonglearning. mendelu.cz/ media/pdf/LLL_20201001057.pdf

7. Dofková Radka, Nocar David, ZdráhaL Tomáš (2019) Reflexe připravenosti budoucích učitelů 1. stupně zš používat digitální technologie ve výuce matematiky. Elementary Mathematics Education Journal, 2019, Vol. 1, No. 2. URL: https:// emejournal. upol.cz/Issues/Vol1No2/Dofkova-Nocar-Zdrahal_2019_Vol1No2.pdf

8. BMBF DigitalPakt Schule. URL: https://www.digitalpaktschule.de/index.html

9. Communities of Practice NRW] für eine Innovative. URL: https://comein.nrw/

10. Digitales Kompetenzzentrum für Lehrerbildung in Sachsen. URL: https:// www.zls.uni-leipzig.de/praxisdigitalis/dikolis

УДК 37.091.33:004

ПЕДАГОГІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ ПІД ЧАС ВІЙСЬКОВОЇ АГРЕСІЇ

Андрій ХАРЧУК
Олександр ВОРОБЙОВ
Інститут післядипломної освіти Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The modern development of information technologies opens up new opportunities for improving the educational process, while requiring specific methodological approaches. The article considers the main ways of applying information technologies in educational institutions, in particular the creation of information environments, the use of pedagogical software, multimedia resources, distance courses and websites. The key problems of introducing information technologies into the educational process are identified, in particular the humanization of education, the training of pedagogical personnel and the integration of subjects. The importance of using modern information and communication technologies in martial law to ensure the continuity of education and the organization of training in shelters is particularly emphasized.*

Keywords: *information technologies, educational process, distance learning, pedagogical software, humanization of education, multimedia tools, technical means, martial law, shelter, information culture.*

Анотація. *Сучасний розвиток інформаційних технологій відкриває нові можливості для удосконалення освітнього процесу, вимагаючи при цьому специфічних методичних підходів. У статті розглянуто основні шляхи застосування інформаційних технологій у навчальних закладах, зокрема створення інформаційних середовищ, використання педагогічних програмних засобів, мультимедійних ресурсів, дистанційних курсів та вебсайтів. Визначено ключові проблеми впровадження інформаційних технологій у навчальний процес, зокрема гуманітаризацію освіти, підготовку педагогічних кадрів та інтеграцію предметів. Окремо наголошено на важливості використання*

сучасних інформаційно-комунікаційних технологій в умовах воєнного стану для забезпечення безперервності освіти та організації навчання в укриттях.

Ключові слова: *інформаційні технології, навчальний процес, дистанційне навчання, педагогічні програмні засоби, гуманітаризація освіти, мультимедійні засоби, технічні засоби, воєнний стан, укриття, інформаційна культура.*

Сучасний розвиток інформаційних технологій та їх використання в освіті вимагає специфічних методичних підходів. Цій проблематиці присвячено чимало наукових праць. Проте проблема залишається актуальною і сьогодні потребує подальшого наукового осмислення.

Під інформаційними технологіями розуміється процес використання засобів і методів збору, обробки та передачі даних для отримання нової інформації про стан об'єкта, процесу чи явища.

Сьогодні виділяють основні шляхи застосування інформаційних технологій в освіті:

– створення інформаційних середовищ навчальних закладів;

– розробка педагогічних програмних засобів (ППЗ);

– застосування інформаційно-комунікаційних технологій під час здійснення проєктивного і дослідницького навчання;

– використання мультимедійних засобів навчання;

– розробка дистанційних курсів;

– застосування інформаційних технологій в управлінні навчальними закладами;

– використання засобів Інтернету для пошуку інформації, розробки програмно-методичного забезпечення, професійного та психологічного консультування;

– створення вебсайтів навчальних закладів;

– здійснення профорієнтаційної роботи;

– розробка та використання контролюючих програмних продуктів;

– створення електронних бібліотек, медіатек тощо [1].

Впровадження інформаційних технологій у навчальний процес викликає низку проблем, що стосуються змісту, методів, організаційних форм та засобів навчання. Особливу увагу слід приділити гуманітаризації освіти, інтеграції навчальних предметів, фундаменталізації знань, підготовці та вдосконаленню педагогічних кадрів. Важливим аспектом є створення системи безперервної освіти, зокрема самоосвіти, яка забезпечує оволодіння основами сучасної інформаційної культури [3].

Сучасні революційні зміни в інформаційних технологіях вимагають нових підходів до професійної підготовки спеціалістів у різних галузях, зокрема в сфері служби цивільного захисту.

В умовах війни з російською федерацією необхідно поєднувати комплекс різноманітних освітніх та інформаційних технологій для ефективної

реалізації якісного дистанційного навчання та забезпечення безперервності освітнього процесу в надзвичайних ситуаціях.

Особливу увагу слід приділити організації та переведення освітнього процесу у спеціально підготовлених приміщеннях для укриття, з використанням технічних засобів та інформаційних мереж.

Інформаційні джерела

1. Інформаційні технології в освіті. URL: https://allreferat.com.ua/uk/pedagogika_metoduka_vukladanny/kontrolnaya/5888

2. Сергієнко Т. І. Вплив сучасної освіти на сталий розвиток суспільства. Освіта як чинних формування креативних компетентностей в умовах цифрового суспільства. Матеріали Міжнародної науково практичної конференції (27–28 листопада 2019 року, м. Запоріжжя). Запоріжжя: ЗНУ, 2019. С. 150–152.

3. Шаров С. В. Розробка інформаційної системи з навчально-виробничих практик. Фізико-математична освіта. 2017. №º 3. С. 194–198.

УДК 614.841

ВІРТУАЛЬНІ СИМУЛЯТОРИ ДЛЯ НАВЧАННЯ ПРАВИЛАМ ЕВАКУАЦІЇ

Діана ПАВЛОВСЬКА
Руслан ПАРХОМЕНКО
Кафедра пожежної тактики та аварійно-рятувальних робіт Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *This work focuses on the use of virtual simulators for training the population to respond to emergency situations. With the increasing number of technological and military threats, implementing innovative training methods has become highly relevant. Virtual simulators enable individuals to practice actions in a safe environment, simulating realistic scenarios such as fires, earthquakes, and other emergencies. Due to their accessibility, scalability, and interactivity, these technologies help develop essential skills without risking lives. The paper examines examples like the VR Fire Extinguishing Experience Simulator, RescueSim, Escape Room VR, and Pathfinder, demonstrating the practicality and efficiency of this approach. Implementing such solutions enhances public awareness and psychological readiness, which is crucial for modern society.*

Keywords: *virtual simulators, evacuation, emergency situations, VR Fire Extinguishing Experience Simulator, VR Fire Drill Trainer, RescueSim, Escape Room VR, Pathfinder.*

Анотація. *Ця робота присвячена використанню віртуальних симуляторів для підготовки населення до дій у надзвичайних ситуаціях. У зв'язку зі зростанням кількості техногенних та воєнних небезпек особливо актуальним стає впровадження інноваційних методів навчання. Віртуальні симулятори дозволяють відпрацьовувати дії у безпечному середовищі, створюючи реалістичні сценарії, що імітують пожежі, землет-*

руси та інші НС. Завдяки своїй доступності, масштабованості та інтерактивності, ці технології допомагають формувати навички без ризику для життя. У роботі розглянуто приклади таких систем, як VR Fire Extinguishing Experience Simulator, RescueSim, Escape Room VR і Pathfinder, які демонструють практичність і ефективність підходу. Впровадження подібних рішень підвищує обізнаність та психологічну готовність населення, що є важливим для сучасного суспільства.

Ключові слова: *віртуальні симулятори, евакуація, надзвичайні ситуації, VR Fire Extinguishing Experience Simulator, VR Fire Drill Trainer, RescueSim, Escape Room VR, Pathfinder.*

Впродовж останніх років спостерігається тенденція збільшення кількості надзвичайних ситуацій (далі НС) техногенного, а з 2022 року – воєнного характеру: пожежі, можливість дії вибухової хвилі при повітряних обстрілах, біологічного, хімічного та радіаційного уражень, які є джерелом ураження і загибелі людей у громадських місцях.

Одним із видів захисту від негативного впливу будь-яких НС є проведення процесу своєчасної і швидкої евакуації із зони дії НС, ефективність якої залежить від ступеня підготовленості працівників та персоналу, а швидке виконання евакуаційних заходів можливе за умови завчасної і періодичної підготовки. Вона передбачає проведення інструктажів, навчання та тренувань для усіх працівників та самопідготовки для незайнятих верств населення, періодичність проведення яких регламентується законодавством, проте кількість травмованих показує тенденцію до їх зростання.

Водночас, проведення додаткових навчань у реальних умовах стикається з низкою труднощів, серед яких – обмежені ресурси, небезпечні умови та низький рівень зацікавленості громадян у засвоєнні необхідних знань і навичок. У зв'язку з цим виникає необхідність у впровадженні інноваційних підходів, таких як використання технологій віртуальної реальності, для навчання населення правилам поведінки та діям у надзвичайних ситуаціях. Це дозволить підвищити ефективність підготовки, створюючи безпечні умови для тренувань і моделюючи реалістичні сценарії.

Віртуальні симулятори для навчання правилам евакуації – це сучасний інструмент, який допомагає навчати людей правильно реагувати на надзвичайні ситуації, такі як пожежі, землетруси, або інші небезпечні події. Завдяки імітації реальних сценаріїв у безпечному віртуальному середовищі, вони дозволяють відпрацювати необхідні навички без ризику для життя. Особливостями віртуальних симуляторів є їхня реалістичність, так як віртуальні симулятори відтворюють умови реального життя, *наприклад*, поведінку вогню, дим, звукові та візуальні ефекти, які створюють стресову обстановку. Також учасники можуть проходити різні сценарії, *наприклад*, евакуацію зі школи, офісу, торгового центру, чи навіть метро. Інтерактивність є однією з особливостей, оскільки в симуляторах користувачі приймають рішення в реальному часі, що допомагає відпрацювати певні алгоритми дій. І також однією з головних осо-

бливостей є аналіз результатів. Після завершення тренування система аналізує дії учасників, показуючи їхні помилки та правильні кроки.

Перевагами використання віртуальних симуляторів для навчання правилам евакуації є безпечне навчання, та як люди навчаються правильно реагувати в екстремальних умовах без ризику для власного життя. Ще одними позитивних факторів можна вважати – економію ресурсів, оскільки використання віртуальних технологій обходиться дешевше, ніж реальні тренувальні полігони, та масштабованість, оскільки можна навчати одночасно велику кількість людей.

Навчальна система віртуальної реальності VR Fire Extinguishing Experience Simulator навчить всіх бажаючих, як потрібно себе вести під час пожежі. За її розробку взялися компанії NEC і MX Mobiling Co Ltd. Система працює на базі Galaxy Gear VR, де в якості дисплея можна використовувати смартфони компанії виробника Samsung, а для управління створено спеціальний контролер у вигляді вогнегасника. Такий симулятор моделює пожежу в закритих приміщення і на відкритому повітрі. Контролює пожежу спеціальний комп'ютер зі необхідним програмним забезпеченням (ПЗ), який створює реалістичну поведінка вогню, який палає навколо, контролює вітер і дим. Зараз доступна ситуація пожежі в офісі, в майбутньому буде додана кухня, квартира і деякі виробничі приміщення.

Одним з прикладів сучасних симуляторів є VR Fire Drill Trainer. Однією з ключових переваг VR Fire Drill Trainer є його доступність та безпека. Традиційна пожежна підготовка часто пов'язана зі значними витратами, логістичними проблемами та екологічними проблемами через використання хімічних речовин та живого полум'я. За допомогою багаторазової системи VR слухачі можуть практикуватися кілька разів, відточуючи свої навички в різних сценаріях пожежі, і все це без шкоди навколишньому середовищу або не вимагаючи спеціалізованого обладнання. Також виробник пропонує власний унікальний інноваційний симулятор вогнегасника, який розроблений для відпрацювання навичок гасіння вогню первинними засобами пожежогасіння і дозволяє навчитися гасінню пожеж різних класів з різними типами вогнегасників без перезарядки і в безпечних та комфортних умовах.

RescueSim – це провідна інтерактивна онлайн-навчальна платформа, що дозволяє тренувати рятувальників з надання першої допомоги населенню у разі виникнення надзвичайної ситуації. Ця платформа є більш спрямованою для навчання рятувальників, але всі охочі цивільні також можуть пройти ці навчання та отримати певний досвід та знання як діяти в надзвичайних ситуаціях різного характеру.

Escape Room VR – це навчання правилам евакуації через ігрові завдання, які роблять процес інтерактивним і цікавим. Такі навчання можуть проходити, як дорослі так і діти, оскільки навчання проходить виконуючи певні завдання в ігровій формі, що допомагає ще більш заохочувати різні вікові

категорії для навчання, які просто необхідні в сьогоденні. Це досягається за рахунок інтерактивного занурення населення в різні сценарії позаштатних ситуацій і надання емоційного ефекту з використанням комп'ютерної симуляції у віртуальній реальності.

Але не тільки навчання населення є важливим при евакуації під час НС. Важливою частиною евакуації є все ж таки правильний розрахунок маршрутів та часу евакуації. І в цьому може бути корисною програма Pathfinder. Це програма, яка реалізує індивідуальну модель руху людей при евакуації. Програма має графічний інтерфейс для завдання вихідних даних, а також інструменти для 2D і 3D-візуалізації результатів. Використання програмного комплексу Pathfinder дозволяє моделювати евакуацію у різних будівлях та приміщеннях, є можливість налаштовувати конкретний розрахунок з усіма можливими факторами: моделювання евакуації людей з обмеженими можливостями; здатність задання та коригування швидкості агентів на різних ділянках шляху евакуації; наявність функції, котра регулює початок руху агентів в заданій поведінці тощо. Завдяки 2D і 3D-візуалізації результатів можна навчати населення де і як можна покидати те чи інше приміщення, щоб мінімізувати шкоду для себе та оточуючих.

Висновки. Отже, основною причиною незацікавленості населення є впевненість відвідувачів громадських місць у тому, що технічні системи безпеки об'єкта та його персонал захистять їх від негативного впливу надзвичайних ситуацій. Доцільність підвищення безпеки громадських місць у надзвичайних ситуаціях шляхом впровадження запропонованих інноваційних рішень для галузі цивільної безпеки з використанням програмних продуктів віртуальної реальності на гаджетах відвідувачів і системи мотивації у вигляді бонусних пропозицій є беззаперечною. Отже, можна стверджувати, що застосування віртуальної реальності в проєктах системи захисту населення сприяє підвищенню рівня знань і психологічної підготовленості населення до дій при виникненні надзвичайних ситуацій.

Інформаційні джерела

1. Бондар Д. В., Гурник А. В., Литовченко А. О., Хижняк В. В., Шевченко В. Л., Ядченко Д. М. Застосування безпілотних авіаційних систем у сфері цивільного захисту. Київ, 2022. С. 312.

2. Візуалізація інформації: що, чому, навіщо, як. URL: https://yur-gazeta.com/golovna/vizualizaciya-informaciyi-shcho-chomu-navishcho-yak.html.

3. Морозова Д. М., Отрош Ю. А., Рибка Є. О., Тригуб В. В. Розбір функціональних характеристик програми Pathfinder: матеріали міжнародної науково-практичної конференції "Problems of Emergency Situations". Харків: НУЦЗ України, 19 травня 2022. URL: https://nuczu.edu.ua/images/topmenu/science/konferentsii/2022/2.pdf

4. Liu J., Zhang R., Yan W., & Sun L. (2021, June). Evacuation of building fire personnel based on BIM+ GIS: A review. In IOP Conference Series: Earth and Environmental Science (Vol. 787, No. 1, p. 012173). IOP Publishing.

УДК 614.841

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ НАВЧАННЯ ПОЖЕЖНІЙ БЕЗПЕЦІ

Ілона МУХА
Володимир-Петро ПАРХОМЕНКО
Руслан ПАРХОМЕНКО
Кафедра пожежної тактики та аварійно-рятувальних робіт Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *The article explores the relevance of integrating artificial intelligence (AI) technologies into fire safety training. The shortcomings of traditional training methods are substantiated, and innovative approaches are proposed, including interactive simulations, personalized learning, risk analysis, and automated knowledge monitoring. The application of AI enhances the quality and effectiveness of training by ensuring its personalization and adaptability to modern challenges. The technological capabilities are examined, including the use of virtual and augmented reality, big data analysis, and risk forecasting. It is concluded that AI holds significant potential for reducing human and material losses in emergency situations.*

Keywords: *fire safety, artificial intelligence, interactive training, simulations, risk analysis, virtual reality, augmented reality, automation.*

Анотація. *У статті розглядається актуальність впровадження технологій штучного інтелекту (ШІ) у навчання пожежній безпеці. Обґрунтовано недоліки традиційних методів підготовки та запропоновано інноваційні підходи, що включають інтерактивні симуляції, індивідуалізоване навчання, аналіз ризиків і автоматизацію моніторингу знань. Застосування ШІ дозволяє підвищити якість та ефективність навчання, забезпечуючи його персоналізацію та адаптивність до сучасних викликів. Розглянуто технологічні можливості, зокрема використання віртуальної та доповненої реальності, аналіз великих даних і прогнозування ризиків. Зроблено висновок про значний потенціал ШІ для зниження людських і матеріальних втрат у разі надзвичайних ситуацій.*

Ключові слова: *пожежна безпека, штучний інтелект, інтерактивне навчання, симуляції, аналіз ризиків, віртуальна реальність, доповнена реальність, автоматизація.*

У сучасному світі, де технології стрімко розвиваються, пожежна безпека залишається одним із ключових аспектів захисту життя та майна. Щороку тисячі пожеж завдають значних людських та економічних втрат. Основним способом зниження ризиків є якісне навчання працівників служб порятунку, промислових працівників, а також усіх верств населення. Проте традиційні методи навчання втрачають ефективність через демонстрацію практичної орієнтації, інтерактивності та адаптивності. На допомогу приходять технології штучного інтелекту (ШІ), які дозволяють створити інноваційні підходи до навчання, виробляючи його персоналізованим, ефективним і реалістич-

ним. ШІ може бути використаний для побудови систем навчання, які базуються на симуляціях, адаптації до рівня знань та аналізу ризиків. без підвищення рівня знань, такі технології допомагають зменшити людські та матеріальні втрати ефективною підготовкою до надзвичайних ситуацій.

Актуальність інтеграції ШІ у пожежну безпеку. Навчання пожежній безпеці завжди було основним аспектом роботи служб порятунку та освітніх установ. В умовах сучасного світу зростає кількість деяких загроз: від промислових пожеж до лісових пожеж, спричинених зміною клімату. Швидке реагування, правильні дії та розуміння ризиків можуть врятувати життя. Традиційні методи навчання, такі як лекції, відео-уроки або тренінги, часто є недостатньо ефективними, оскільки не забезпечують практичних навичок для реальних ситуацій. ШІ дозволяє подолати ці обмеження, створюючи адаптивні системи навчання, які включають інтерактивні симуляції, автоматизовану перевірку знань і прогнозування наявних загроз. Це не зменшує вартість навчання, а й значно знижує його якість та практичність.

Технологічні можливості ШІ в навчанні пожежній безпеці:

1. Реалістичні симуляції для тренувань

ШІ дозволяє моделювати різноманітні сценарії пожежі за допомогою віртуальної реальності (VR) та доповненої реальності (AR).

У віртуальному середовищі можна моделювати пожежу у багатоповерховому будинку, фабриці чи лісі. Учасники навчання можуть відпрацьовувати евакуацію, пошук постраждалих або боротьбу з вогнем. Доповнена реальність дозволяє відтворювати пожежі в реальних приміщеннях з використанням цифрових накладень, що додає елемент інтерактивності. Це не лише реалістичність навчання, а й дозволяє тренувати людей у безпечних умовах.

2. Індивідуалізоване навчання

Системи ШІ здатні аналізувати знання кожного учасника та адаптувати навчальний процес до його потреб.

Якщо працівник не до кінця використовує принципи використання вогнегасників, система може запропонувати додаткові матеріали чи моделювання. Машинне навчання дозволяє виявляти прогалини у знаннях та під кінцевий контент відповідно до рівня підготовки.

3. Аналіз даних та прогнозування ризиків

Системи на основі ШІ можуть обробляти великі обсяги даних для прогнозування пожежних ризиків.

Аналіз метеорологічних умов дозволяє визначити ймовірність виникнення лісових пожеж. На підприємствах ШІ можна аналізувати стан обладнання та виявляти видимо небезпечні ділянки. Такі системи можуть бути інтегровані в навчання, допомагаючи учасникам краще зрозуміти, як оцінювати ризики та діяти на випередження.

4. Автоматизація моніторингу та оцінки знань

ШІ забезпечує автоматичну перевірку знань та аналіз дій учасників у симуляціях.

Висновки. Отже, система може оцінити, наскільки швидко учасник правильно відреагував на змодельовану швидкість. Автоматизовані тести та тренінги не дозволяють отримувати миттєвий зворотний зв'язок. А це вже є завданням викладачів зосередитися на індивідуальному супроводі, а не на рутинній роботі.

Інформаційні джерела

1. Musaev A., Parwez M., & Zaslavsky A. (2018). Real-time Personalization of Emergency Training with AI-driven Simulations. Journal of Safety Science, 105, pp. 134–140.

2. Garcia L., Sanchez P., & Martínez F. (2021). AI Applications in Fire Safety Management: From Risk Prediction to Training Simulations. Safety and Health at Work, 12(3), pp. 246–255.

3. Rahman S., & Chan A. (2020). Virtual and Augmented Reality in Fire Safety Training: A Systematic Review. International Journal of Safety Science, 123, pp. 112–125.

УДК 614.841

ЦИФРОВІЗАЦІЯ ПРОГРАМ НАВЧАННЯ Д ЛЯ ПОЖЕЖНИХ-РЯТУВАЛЬНИКІВ

Галина АЛЬФАВІЦЬКА
Володимир-Петро ПАРХОМЕНКО
Руслан ПАРХОМЕНКО
Кафедра пожежної тактики та аварійно-рятувальних робіт Львівського державного університету безпеки життєдіяльності, м. Львів, Україна.

Abstract. *This paper aims to explore the main directions of digitalization in the training of firefighting rescuers, as well as analyze specific examples of successful implementation of innovative solutions in this field. Attention is given to tools such as the FlameSim and FireRescue1 Academy platforms, the Responder Safety Learning Network mobile application, and VR technologies implemented in the FLAIM Trainer program. The study emphasizes the importance of digitalization in enhancing training efficiency, improving the safety of rescuers, and reducing risks in their work processes*

Keywords: *digitalization of education, learning efficiency, safety, innovative solutions, the FlameSim platform, FireRescue1 Academy, Responder Safety Learning Network, VR technologies, the FLAIM Trainer program.*

Анотація. *Цей реферат має на меті дослідити основні напрями цифровізації навчання пожежних рятувальників, а також проаналізувати конкретні приклади успішного впровадження інноваційних рішень у цій сфері. Увага приділяється таким інструментам, як платформи FlameSim, FireRescue1 Academy, мобільні додатки Responder Safety Learning Network, а також технології VR, що реалізовані у програмі FLAIM Trainer. У дослідженні підкреслюється значення цифровізації для підвищення ефективності навчання, покращення безпеки рятувальників і зниження ризиків у процесі їхньої роботи.*

Ключові слова: *цифровізація навчання, ефективність навчання, безпека, інноваційні рішення, платформа FlameSim, FireRescue1 Academy, Responder Safety Learning Networ, технології VR, програма FLAIM Trainer.*

У сучасному світі, що динамічно змінюється під впливом технологічного прогресу, адаптація до інновацій є важливою умовою для забезпечення ефективності роботи у різних сферах. Однією з таких сфер є пожежна безпека, де потреба у використанні сучасних технологій особливо гостро відчувається через складність і небезпеку роботи рятувальників. Пожежні рятувальники щоденно стикаються з ризиками, які потребують не лише фізичної підготовки, але й високого рівня знань, швидкості прийняття рішень і координації дій у складних умовах.

Традиційні методи навчання, які зосереджені на теоретичній підготовці та практичних тренуваннях, сьогодні вже не в змозі повністю відповідати новим викликам. Швидкість урбанізації, зростання кількості складних техногенних об'єктів, кліматичні зміни, що призводять до масштабних природних катастроф, вимагають від пожежних рятувальників постійного вдосконалення. У цьому контексті цифровізація навчальних програм стає необхідною складовою професійної підготовки.

Цифрові технології не лише доповнюють традиційні методи навчання, але й створюють абсолютно нові можливості для розвитку навичок і знань. Віртуальні тренувальні платформи дозволяють моделювати складні сценарії, які важко відтворити у реальних умовах. Онлайн-курси та вебінари надають доступ до актуальних матеріалів і допомагають пожежним рятувальникам підтримувати високий рівень професійної компетенції незалежно від їхнього місцезнаходження. Мобільні додатки забезпечують швидкий доступ до критично важливої інформації у польових умовах, а технології доповненої та віртуальної реальності дозволяють безпечно практикувати дії у ситуаціях, наближених до реальних.

Цифровізація навчання пожежних рятувальників охоплює кілька ключових напрямків:

– віртуальні тренувальні платформи;
– онлайн-курси та вебінари;
– мобільні додатки;
– використання доповненої реальності (AR) та віртуальної реальності (VR);
– віртуальні тренувальні платформи.

Одним з найефективніших інструментів цифровізації є створення віртуальних тренувальних платформ. Вони дозволяють моделювати різні сценарії надзвичайних ситуацій, що дає можливість рятувальникам практикувати свої навички у безпечному середовищі.

Платформа FlameSim – це передова система моделювання пожежних ситуацій, яка дозволяє створювати реалістичні сценарії пожеж. Вона використовується для тренувань у різних умовах: від квартирних пожеж до масштабних лісових пожеж. FlameSim дозволяє інтерактивно відпрацьовувати тактики гасіння пожеж та координацію дій рятувальників.

Онлайн-курси та вебінари. Завдяки розвитку інтернет-технологій, пожежні рятувальники мають доступ до великої кількості онлайн-курсів та вебінарів, які допомагають підвищувати кваліфікацію без необхідності фізичної присутності.

Платформа FireRescue1 Academy пропонує понад 400 курсів, які охоплюють різні аспекти роботи пожежних рятувальників, включаючи медичну підготовку, тактику гасіння пожеж, лідерство та управління командою. Ці курси дозволяють рятувальникам навчатися у зручний для них час і темп.

Мобільні додатки. Мобільні додатки стають незамінними помічниками для рятувальників, надаючи доступ до критично важливої інформації та навчальних матеріалів у будь-який момент.

Додаток Responder Safety Learning Network – це інтерактивний інструмент, який пропонує навчальні модулі з безпеки на дорозі, стратегії управління ризиками та багато іншого. Додаток забезпечує швидкий доступ до актуальної інформації та інструкцій, що може бути життєво необхідним у надзвичайних ситуаціях.

Використання доповненої реальності (AR) та віртуальної реальності (VR). AR та VR технології відкривають нові горизонти у підготовці пожежних рятувальників, дозволяючи їм зануритися у віртуальні світи, де вони можуть безпечно практикувати складні навички.

Програма FLAIM Trainer використовує VR для створення реалістичних сценаріїв пожеж. Використовуючи спеціальне обладнання, рятувальники можуть відпрацьовувати свої дії у різних умовах: від невеликих пожеж до великих катастроф. Така технологія дозволяє знизити ризики під час реальних тренувань і підвищити ефективність навчання.

Висновки. Цифровізація програм навчання для пожежних рятувальників значно підвищує ефективність підготовки та забезпечує швидкий доступ до необхідних знань і навичок. Використання віртуальних тренувальних платформ, онлайн-курсів, мобільних додатків, а також AR і VR технологій, відкриває нові можливості для розвитку професійних навичок і забезпечення безпеки як рятувальників, так і громадян. Інноваційні підходи до навчання стають запорукою успішної боротьби з надзвичайними ситуаціями у сучасному світі.

Інформаційні джерела

1. FlameSim. URL: https://www.flamesim.com

2. FireRescue1Academy. URL: https://www.firerescue1academy. com

3. Pixaera. Revolutionize Safety Training with Pixaera's Immersive Learning Platform. URL: https://pixaera.com/revolutionalize-your-ehs-training/?utm_source=google&utm_medium=CPC&utm_campaign=tofu&utm_term=safety%20management%20training&utm_term=safety%20management%20training&utm_campaign=ToFu+Europe&utm_source=adwords&utm_medium=ppc&hsa_acc=9521312752&hsa_cam=21828056107&hsa_grp=167732076143&hsa_ad=717672807354&hsa_src=g&hsa_tgt=kwd-80708811&hsa_kw=safety%20management%20training&hsa_ mt=b&hsa_ net=adwords&hsa_ver=3&gad_source=1&gbraid=0AAAAA-MvwtW8WT9rNJvODvq3ENg0OwZ1s&gclid=Cj0KCQiAgJa6BhCOARIsAMiL7V_yW-JIRkkEQky5U85hS28XxlUkAdDJCN0asRGnbaioKF8OL_opIXEaAk0DEALw_wcB

4. Flaim. FLAIM Trainer™, the world's first immersive technology enabled firefighter training solution. URL: https://flaimsystems.com/products/ trainer

З М І С Т

СЕКЦІЯ 1

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

НАПРЯМ 1. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ВІЙНИ

НАПРЯМ 4.
ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

НАПРЯМ 5.
ГЕНДЕР У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

НАПРЯМ 6.
КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

НАПРЯМ 7.
КІБЕРБЕЗПЕКА ІНФРАСТРУКТУРИ

НАПРЯМ 8.
ІНФОРМАЦІЙНІ ВІЙНИ

СЕКЦІЯ 2

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ ВІЙНИ

НАПРЯМ 9.
ПРИКЛАДНЕ ТА СИСТЕМНЕ ПРОГРАМУВАННЯ

НАПРЯМ 10.
МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

НАПРЯМ 11.
3D МОДЕЛЮВАННЯ ТА 3D ДРУК

НАПРЯМ 12.
МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СИСТЕМ

НАПРЯМ 13.
ОРГАНІЗАЦІЯ БАЗ ДАНИХ І ЗНАНЬ

НАПРЯМ 14.
ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ ДАНИХ

НАПРЯМ 15.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРОЄКТАМИ

НАПРЯМ 16.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Наукове видання

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Збірник наукових праць
V Міжнародної науково-практичної конференції
ІБІТ 2024

Відповідальні за випуск **Ростислав ТКАЧУК**

Оригінал-макет **Ростислав ТКАЧУК**

Друк на різографі

Підписано до друку 13.12.2024 р.
Формат 70×100/16. Гарнітура Times New Roman.
Папір офсетний. Друк цифровий.
Ум. друк. арк. 51,68. Обл.-вид. арк. 46,71
Наклад 100 прим.

Видавець і виготовлювач: ТОВ «Растр-7»
79005, м. Львів, вул. Кн. Романа, 9/1.
Тел./факс: (032) 235 72 13. E-mail: rastr.sim@gmail.com
www.rastr-7.com.ua

Свідоцтво суб'єкта видавничої справи
ЛВ № 22 від 19.11.2002 р.

V International Scientific and Practical Conference CYBERSUCURITY AND INFORMATION TECHNOLOGY

CIT 2024

November 27 - 2024 Lviv-Ukraine