Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет «Львівська політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VI Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

30 листопада 2023 року

Львів – 2023

ББК 32.81+78.362

*Інформаційна безпека та інформаційні технології: з*бірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. Львів, ЛДУ БЖД, 2023, 489 с.

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
КІБЕРБЕЗПЕКА

UDC 004.056.5 (043.2)

ANALYSIS OF CYBER THREAT INTELLIGENCE MODELS

Alla Pinchuk, Roman Odarchenko, Oleh Polihenko
National Aviation University, Kyiv

Abstract. Cyber threat intelligence (CTI) is a critical tool for organizations to defend against cyberattacks. CTI models provide a framework for organizing and analyzing CTI data, helping organizations to understand and mitigate potential threats. This paper analyzes three of the most common CTI models: Diamond, MITRE ATT&CK and Unified Kill Chain.

Key words: Cyber Threat Intelligence, Diamond Model, Unified Kill Chain, MITRE ATT&CK

Анотація. Розвідка кіберзагроз є критично важливим інструментом для захисту організацій від кібератак. Моделі розвідки забезпечують основу для організації та аналізу даних щодо кіберзагроз, допомагаючи організаціям зрозуміти та зменшити потенційні загрози. У цій роботі проаналізовано три найпоширеніші моделі: Diamond, MITRE ATT&CK та Unified Kill Chain.

Ключові слова: розвідка кіберзагроз, Diamond, Unified Kill Chain, MITRE ATT&CK

CTI is an essential cybersecurity tool that helps organizations collect, analyze, and share cyber threat information to proactively protect against cyberattacks. CTI models enable organizations to effectively organize and analyze CTI data, gaining a comprehensive understanding of the evolving threat landscape.

In this article, three of the most common CTI models were analyzed:

- Diamond Model;
- MITRE ATT&CK Model;
- Unified Kill Chain Model.

Diamond Model. This model illustrates cyber threats by focusing on four key elements which showed on the Figure 1.

It emphasizes the relationships between these elements to provide a comprehensive understanding of cyber incidents. By examining these connections, security professionals gain insights into an attacker's tactics, techniques, and procedures (TTPs), aiding in threat detection, response, and attribution. In general, it helps to correlate and contextualize information about threats [1-2].

Key aspects:

- ability to easily pivot from one piece of intelligence to another, which helps either fulfill the full picture while gathering, or show "blindspots" in intelligence;
- ability to form activity groups and activity-attack graphs.

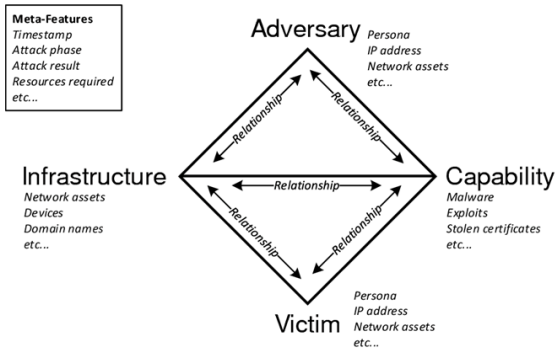


Figure 1 – Diamond Model

MITRE ATT&CK Model. This model is based on real-world events and contains information about the tactics, techniques, sub-techniques and procedures used by threat actors. The information in the MITRE ATT&CK knowledge base is presented as a set of matrices [3-5].

Some of the key aspects:

- *Comprehensiveness:* the model covers a wide range of adversary TTPs.
- *Granularity:* the model is very granular, providing detailed information about each technique.
- *Community-driven:* the model is maintained by a community of experts, which ensures that it is always up-to-date with the latest threat intelligence.

Unified Kill Chain Model. The Unified Kill Chain extends and combines existing models: Lockheed Martins' Cyber Kill Chain and MITRE's ATT&CK for Enterprise. This model includes 18 tactics that can be used to describe the phases of modern cyberattacks. [6]. Model has unique approach, it divided into 3 phases (Fig.2):

- *Initial Foothold (In):* compromise a system to gain access to network.
- *Network Propagation (Through):* gain additional access within network.
- *Action on Objectives (Out):* achieve goal of attack [7].

Figure 2 – Unified Kill Chain approach

Key aspects:

- the Unified Kill Chain is an ordered arrangement of 18 unique attack phases that may occur in end-to-end cyberattack;
- it covers activities that occur outside and within the defended network.

Analysis. All of the above models are all useful tools for understanding and responding to cyber threats. Thus, we can make the next conclusion about each model:

- *Diamond Model:* simple and easy-to-understand model that is well-suited for organizations that need a general understanding of the cyber attack lifecycle;
- *Unified Kill Chain Model:* more detailed model that is better suited for organizations that need to track the progress of attacks in more detail;
- *MITRE ATT&CK Model:* the most comprehensive model and is best suited for organizations that need to identify specific TTPs that could be used to attack them.

Conclusions. The landscape of cyber threats is complex and ever-evolving. Each CTI model offers unique perspectives and methodologies to analyze, understand, and mitigate these threats. Combining multiple models or frameworks often yields a more holistic and effective approach to cybersecurity, enabling organizations to proactively defend against a diverse range of cyber threats. Continuous evolution and adaptation of these models are essential to stay ahead in the ongoing battle against cyber adversaries.

References

1. Warner C. Diamond Model in Cyber Threat Intelligence. *Medium.* URL: https://warnerchad.medium.com/diamond-model-for-cti-5aba5ba5585.

2. Strategies for Gathering and Contextualizing Cyber Threat Intelligence. *Netskope.* URL: https://www.netskope.com/blog/strategies-for-gathering-and-contextualizing-cyber-threat-intelligence.

3. Nickels K. Using ATT&CK to Advance Cyber Threat Intelligence – Part 1. *Medium.* URL: https://medium.com/mitre-attack/using-att-ck-to-advance-cyber-threat-intelligence-part-1-c5ad14d59724.

4. Warner C. MITRE ATT&CK in Cyber Threat Intelligence. *Medium.* URL: https://warnerchad.medium.com/mitre-att-ck-for-cti-5c267dca59c2.

5. What is the Mitre Att&ck Framework? - CrowdStrike. *crowdstrike.com.* URL: https://www.crowdstrike.com/cybersecurity-101/mitre-attack-framework/.

6. The Unified Kill Chain. Unified Kill Chain: Raising Resilience Against Cyber Attacks. URL: https://www.unifiedkillchain.com/.

7. Understanding Cyber Kill Chain, MITRE ATT&CK Framework and Unified Kill Chain. *Medium.* URL: https://medium.com/@wintersoldiers/understanding-cyber-kill-chain-mitre-att-ck-framework-and-unified-kill-chain-f306ceca19be.

UDC 004.6+665.1

BIOMETRIC INFORMATION SECURITY IN PRINTING INDUSTRY

Vytak Andrii
Ukrainian Academy of Printing, Lviv

Визначено особливості взаємодії між безпекою біометричної інформації та потоками даних поліграфічної промисловості. Виконано аналіз напрямків інтеграції біометричних технологій в корпоративний процес управління документами, контролю доступу та загальної безпеки даних поліграфічних підприємств.

Ключові слова: безпека біометричної інформації, поліграфічна галузь, набір із засобів розробки.

The peculiarities of interaction between of biometric information security and data flows of printing industry have been determined. An analysis of directions of biometric technologies integration into corporate process of document management, access control and general data security of printing enterprises was performed.

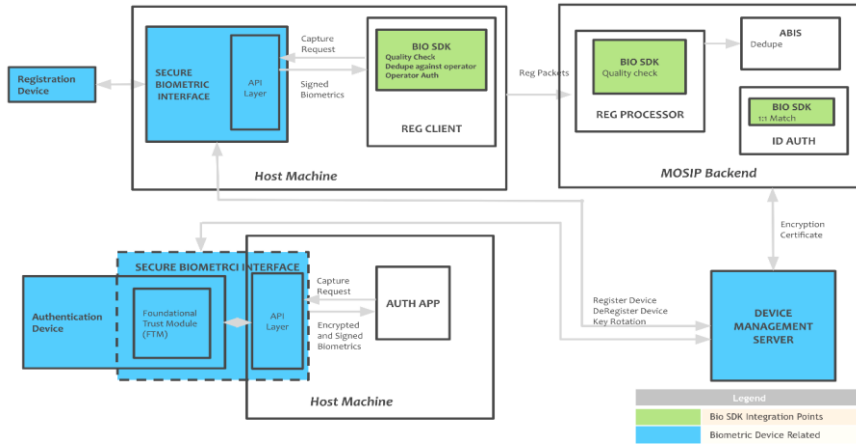
Keywords: security of biometric information, printing industry, software development kit.

In the realm of technological innovation, the printing industry stands as a dynamic player undergoing its own transformative evolution. As businesses increasingly rely on digital platforms for document management, communication, and data storage, the printing industry finds itself at the intersection of traditional and cutting-edge technologies [1]. Against this backdrop, the integration of biometric information security becomes a crucial element in ensuring the confidentiality and integrity of sensitive data within the printing landscape. In a sector where the exchange of confidential documents is commonplace, biometric authentication offers a powerful solution to mitigate the risks associated with unauthorized access. Sensitive documents are not only securely stored but can also be accessed or released for printing only by individuals with the proper biometric credentials. This not only streamlines workflow processes but also adds an extra layer of protection against data breaches. This exploration will navigate the synergies between biometric information security and the printing industry, shedding light on how biometric technologies are reshaping document management, access control, and overall data security. From safeguarding intellectual property to ensuring compliance with regulatory frameworks, the fusion of biometrics and printing technology emerges as a pivotal aspect of modern information management strategies.

In navigating the convergence of biometric information security and the printing industry, a multifaceted set of challenges emerges, each requiring nuanced solutions for successful implementation. One of the central concerns is the need to maintain a delicate equilibrium between heightened security protocols and operational efficiency within the printing workflow. Integrating biometric authentication seamlessly into existing printing infrastructures poses a substan-

tial hurdle. Print environments are often characterized by diverse hardware, software, and user interfaces. The challenge lies not only in the development of compatible technologies but also in the user-friendly implementation that does not impede the speed and ease of traditional printing processes. The success of any security measure hinges on user acceptance and adoption. In the context of the printing industry, where users may range from tech-savvy professionals to those less familiar with advanced technologies, designing an intuitive and user-friendly biometric authentication process becomes paramount. Striking the right balance between robust security and user convenience is crucial to prevent resistance to adoption and ensure the technology's effective use.

The collection, storage, and use of biometric data introduce ethical considerations and privacy concerns. Users must trust that their biometric information is handled securely and ethically. Implementing stringent security measures to protect this sensitive data is imperative, and clear policies and regulations must be established to address privacy concerns. Striking a balance between the need for enhanced security and the protection of user privacy represents a nuanced challenge in this landscape. The printing industry is dynamic, with ever-evolving technologies and shifting business needs. A challenge arises in designing biometric systems that are not only effective in the current context but are also scalable and flexible enough to adapt to future changes in printing technology and workflow requirements [2]. This requires forward-thinking solutions that can accommodate the industry's evolution without necessitating frequent and disruptive system overhauls (figure 1).



In the quest to fortify data protection within the printing industry, the Biometric SDK emerges as a pivotal instrument, seamlessly integrating biometric security measures into existing infrastructures. At its core, the Biometric SDK serves as the bridge between the printing infrastructure and biometric hardware.

During the initialization phase, the SDK establishes a robust connection, ensuring seamless communication and compatibility. This step is foundational, laying the groundwork for subsequent interactions with the biometric ecosystem. The first point of interaction with the printing environment is the isSupported method. This method undertakes a comprehensive assessment, examining both the device and the installed SDK to determine the system's capacity for supporting biometric authentication. Its role is crucial in providing a clear indication of whether the hardware is equipped to engage in the biometric security measures proposed by the SDK. Upon the completion of the authentication simulation, the Biometric SDK invokes a result callback function. This callback mechanism provides crucial feedback to the calling application, conveying whether the biometric authentication was successful or if any issues were encountered during the process. The result callback is instrumental in informing subsequent actions, such as allowing access to sensitive information or triggering printing processes.

In unpredictable landscape of biometric authentication, robust error handling becomes imperative. The Biometric SDK is equipped with mechanisms to address a myriad of issues, including failed biometric recognition, hardware malfunctions, or communication errors. This ensures that authentication process is not only accurate but also resilient in the face of unforeseen challenges. Security is paramount in realm of biometric information. The SDK incorporates a security measures suite to safeguard sensitive biometric data. This includes encryption protocols to protect data during transmission and storage, adherence to stringent privacy regulations, and the enforcement of strict access controls. These measures collectively create a secure environment for handling and managing biometric information. Recognizing the technology dynamic nature, the Biometric SDK is designed with modularity and upgradability in mind. Its modular architecture allows for seamless updates, ensuring compatibility with evolving biometric technologies. This forward-thinking approach guarantees that the SDK remains adaptable to future advancements, contributing to the long-term scalability of entire biometric security framework. In essence, the Biometric SDK serves as a linchpin in the integration of biometric information security within printing industry. Its intricate functionalities, coupled with commitment to security and adaptability, position it as a transformative force. By seamlessly incorporating this SDK into security framework, printing organizations can not only address the challenges posed by biometric integration but also embrace a future where the fusion of biometrics and printing security creates a resilient, efficient, and ethically sound ecosystem.

Reference

1. Durnyak B., Shepita, P., Tupychak, L. Protection of the Information System of the Printing Enterprise from Cyber Threats. CEUR Workshop Proceedings, Vol. 3373, 2023. P. 464–474.

2. Vytak A. Researching of areas the improvement and application areas of robotics vision systems. Ecology and rational nature management. Vol. 1, 2023. P. 345–347.

ЯК ПОДБАТИ ПРО БЕЗПЕКУ ДАНИХ ПРИ КОРИСТУВАННІ ХМАРНИМИ ТЕХНОЛОГІЯМИ

Атаманова Руслана
Вище професійне училище Львівського державного університету безпеки життєдіяльності (м. Вінниця)

Анотація: Тези доповіді містять інформацію про важливість хмарних сервісів та основні проблеми безпеки, які можуть виникнути при роботі з даними та серверами у хмарі. Висвітлено основні правила, які допоможуть зменшити загрози та забезпечити надійне зберігання даних у хмарних сервісах.
Ключові слова: хмарне середовище, проблеми безпеки, комплексне середовище, акаунт, аутентифікація.

Abstract: The abstracts of the report contain information about the importance of cloud services and the main security problems that may arise when working with data and servers in the cloud. The main rules that will help reduce threats and ensure reliable data storage in cloud services are highlighted.
Keywords: cloud environment, security issues, complex environment, account, authentication.

Немає сумнівів в тому, що сьогодні хмарні технології є одними із популярних сервісів для зберігання даних та розміщення серверів цілих компаній. Така популярність пояснюється зручністю та доступністю до даних з будь-якого місця чи пристрою, відносною дешевизною, можливістю одночасної онлайн роботи декількох користувачів, наявністю засобу аварійного відновлення та інших переваг. Але якщо не створити належний захист та налаштування безпеки даних, то це стає цілю для кіберзлочинців, які після отримання доступу до даних можуть викрасти конфіденційну інформацію та опублікувати її, а після цього знищити вміст хмарної бази даних. За даними експертів, після початку повномасштабного вторгнення росії на Україну кількість атак та несанкціонованого доступу на хмарні сервіси значно зросла і продовжує зростати.

Здебільшого користувачі допускають помилок у безпеці в самих налаштуваннях хмари та бази даних. Після таких помилок їх можна легко знайти та відсканувати за допомогою різних інструментів. За даними дослідження14 % мобільних додатків (понад мільйона), які у своїй серверній частині мають загальнодоступний хмарний сервіс, через неправильні налаштування хмари розкривали персональну інформацію користувачів. Найпоширенішими помилками в налаштуванні є відсутність контролю та обмеження доступу, наявність багатьох дозволів в груповій політиці безпеки, некоректність у способах підключення до Інтернету, помилки в налаштуваннях віртуалізованих функцій мережі[1].

Корпорація Microsoft серед основних проблем безпеки хмари виділяє такі як:

- **недостатня видимість даних** – пов'язана з віддаленим доступом або використання іншої, а не корпоративної мережі та використання власних пристроїв для доступу до корпоративних ресурсів у різних загальнодоступних і приватних хмарах, що заважає відстежити, які служби використовуються та як дані переміщуються в хмарі;
- **комплексні середовища** – розгортання інфраструктури і програм дають змогу працювати в гібридному багатохмарному середовищі, що охоплює локальні, загальнодоступні й приватні хмари, але у такому середовищі часто виникають помилки конфігурації та важко відстежувати загрози бокового зміщення;
- **швидке впровадження інновацій –** розвиток сучасних технологій (штучний інтелект, машинне навчання, Інтернет речей), що ефективніше забезпечують збір та використання даних, застосування процесів DevOps у розробці, використання малокодових та безкодових рішень породжують недолік швидкого впровадження інновацій – ігнорування стандартів безпеки;
- **відповідність вимогам і керування –** клієнти хмарних провайдерів відповідають за забезпечення відповідності своїх робочих процесів власним стандартам, і не завжди це відповідає програмам акредитації хмарних служб;
- **внутрішні загрози** – можуть йти від працівників, які умисно або випадково використовують авторизований доступ для заподіяння шкоди компанії або розголошують дані працівників організації, включаючи крадіжку й шахрайство. [2]

То як необхідно діяти, щоб зберегти свої дані у безпеці? Хоча хмарні провайдери гарантують високий рівень безпеки, є основні правила та заходи, які потрібно вжити для забезпечення безпеки своїх даних.

Серед основних правил фахівці [3] [4] виділяють такі:

1. Використання надійних паролей та двофакторної (чи багатофакторної) аутентифікації.
2. Проведення аудиту і перевірки файлів та загальних папок.
3. Очищення «вже видалених» файлів.
4. Постійна перевірка підключених додатків та облікових записів.
5. Встановлення та оновлення антивірусного та антишпигунського програмного забезпечення.
6. Обмеження прав доступу до серверів.
7. Увімкнення сповіщень та повідомлень про дії в акаунті.

8. Постійне оновлення програмного забезпечення серверів та операційних систем.

9. Деактивація старих пристроїв, на яких все ще є доступ до акаунту.

10. Увімкнення параметрів відновлення облікового запису.

11. Вихід з облікових записів, якщо не працюєте в них.

12. Створення захисту для своїх пристроїв.

13. Створення резервних копій даних на регулярній основі.

Отже, дотримуючись простих правил для роботи в хмарних сервісах Ви подбаєте про безпеку та цілісність Ваших даних, а також будете впевнені в тому, що забезпечили надійний захист від кіберзлочинців та володієте інформаційною культурою в питаннях зберігання даних у хмарних сервісах.

Література

1. Портал інформаційного агентства УНІАН. Режим доступу: https://www.unian.ua/techno/zberigannya-danih-kompaniy-u-hmarnomu-shovishchi-naskilki-ce-narazi-bezpechno-11812803.html (Дата звернення 01.11.2023).

2. Офіційний веб-сайт корпорації Microsoft. Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cloud-security (Дата звернення 04.11.2023).

3. Портал компанії DATAMI. Режим доступу: https://datami.ua/bezpeka-hmarnih-shovishh-i-tehnologij-osnovni-pravila/ (Дата звернення 05.11.2023).

4. Портал української IT компанії КУБ. Режим доступу: https://kub.ua/blog/bezopasnost-v-oblachnyh-tehnologiyah/ (Дата звернення 30.10.2023).

УДК 355.58

ІНФОРМАЦІЙНІ ВІЙНИ

Батюк Віталій
Львівський державний університет безпеки життєдіяльності, м. Львів

Сьогодні поняття «інформаційна війна» набуває прояву соціально-правової природи суспільства. З давніх часів маніпулювання інформацією через психологічний вплив на опонента було одним з найефективніших засобів ведення війни. У сучасному суспільстві інформаційна війна - це непідконтрольний ресурс, який слабо піддається правовій регламентації, тому активно застосовує неправдиву, перекручену інформацію як засіб маніпуляції свідомістю.

Today, the concept of "information war" is becoming a manifestation of the socio-legal nature of society. Since ancient times, manipulation of information through psychological influence on the opponent has been one of the most effective means of warfare. In modern society, information warfare is an uncontrolled resource that is weakly amenable to legal regulation, so it actively uses false, distorted information as a means of manipulating consciousness.

«Хто володіє інформацією, той володіє світом», – сказав колись Уїнстон Черчіль. Дійсно, інформація у сучасному світі – це стратегічний ресурс, контроль над яким відкриває необмежені можливості. Маніпулювання свідомістю людей як форма впливу на них з метою їх контролю була і залишається ефективним засобом політико-правової боротьби. Розвиток інформаційних технологій, всесвітньої інформаційної мережі дав поштовх до виникнення такого виду ведення протистоянь, як інформаційна війна.

Термін “інформаційна війна” став широко застосовуватися американськими військовими фахівцями після завершення операції “Буря в пустелі”, де інформаційна зброя показала свою високу ефективність і поступово набула популярності. 1992 р. Пентагон видав директиву “Інформаційна війна” (TS 3600.1), в якій окреслювалися основні завдання з підготовки до таких воєн. На основі аналізу концепцій інформаційної війни за видами збройних сил Об’єднаний комітет начальників штабів США ухвалив документ “Загальні погляди на період до 2010 року” (Joint Vision 2010), в якому розробив концепцію інформаційної війни. До елементів інформаційної війни американські фахівці віднесли: добування розвідувальної інформації, дезінформування, психологічні операції, фізичне руйнування інформаційних ресурсів супротивника (у тому числі з використанням електромагнітного впливу), напади (фізичні, електронні) на його інформаційну структуру, зараження комп’ютерними вірусами його обчислювальних мереж і систем, проникнення в інформаційні мережі тощо, а також відповідні заходи протидії для захисту власних інформаційних ресурсів [2]

Нова форма ведення війни, "інформаційна війна", визначається тоді, коли одна нація прагне отримати стратегічні важелі над іншою шляхом підриву, зриву або пошкодження інформаційних систем. [1] Саме інформаційні вкиди та підриви передували загостренню відносин, а в подальшому повномасштабному вторгненню Росії на суверенні земні України, Грузії, Нагірного Карабаху, Придністров'ї, Абхазії, Південній Осетії.

Серед найпоширеніших видів інформаційних війн є гібридна війна, адже вона виходить за рамки традиційних понять про ведення бойових дій. Це війна комбінованого характеру, яка перетворюється хитросплетіння політичних інтриг, запеклої боротьби за політико-економічне домінування над країною, за території, ресурси й фінансові потоки. Жертвами ведення такої війни, зазвичай, стають мирні жителі, передусім, найбеззахисніші категорії населення – люди похилого віку, жінки й діти [3]

Одним з механізмів ведення гібридної інформаційної агресії є маніпулювання гендером. Мета – створення певних переконань, вплив на громадську думку, дестабілізація суспільства та збільшення внутрішніх конфліктів. В інформаційному просторі створюються наративи, що підкреслюють різницю між статевими ролями та підштовхують до конфлікту між гендерними групами.

Проявом гібридної війни можна назвати українсько-російську війну, розпочату в 2014 році. Найбільш чітко характер нового типу війни Росія продемонструвала під час насильницької анексії території Автономної Республіки Крим та проведення там псевдо референдуму навесні 2014 р., а згодом – під час вторгнення до східних областей України [4]. Так, Росія використала проти України ряд підривних соціальних технологій, таких як: технологію поділу України на «народні республіки»; технологію створення кримінального натовпу; технологію заколоту і захоплення влади в містах; технологію «референдуму»; технологію «живого щита» та ін. [5]

Протистояння в інформаційних війнах національних масштабів має односторонній характер. Тому першим кроком у боротьбі з інформаційною агресією є реформування законодавсчих актів у сфері інформації. Не менш важливим фактором у протистоянні інформаційній агресії є впровадження державної політики інтелектуального розвитку суспільства, збільшення його розумового потенціалу для протистояння загрозі інформаційного впливу.

Ефективним кроком в інформаційному протистоянні є створення органів фактчекінгу, основною функцією яких є відстеження та перевірка інформаційного простору у державі. В Україні таким органом є Центр протидії дезінформації — робочий орган Ради національної безпеки і оборони України, утворений відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформа-

ційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

Отже, провівши аналіз еволюції та розвитку інформаційних війн, можна зробити висновок, що її основною метою є досягнення інтересів держави-агресора методом інформаційного обеззброєння та дезінформування жертв, досягнення бажаних результатів будь-якою ціною. Незмінними залишаються методи ведення інформаційної боротьби: пропаганда, викривлення фактів, наклепи, психологічні операції, фізичне руйнування інформаційних ресурсів супротивника, зараження комп'ютерними вірусами його обчислювальних мереж і систем, проникнення в інформаційні мережі противника тощо. Альтернативою для боротьби з інформаційною агресією має бути реформування законодавства в сфері інформації; впровадження державної політики «інтелектуального розвитку» суспільства, надійних захист інформаційних ресурсів. Таким чином, є можливість запобігти деструктивному впливу інформаційної зброї на національну безпеку.

Література

1. Жаровська І., Ортинська Н. Інформаційна війна як сучвсне глобалізаційне явище: Вісник Національного університету "Львівська політехніка". Сер. "Юридичні науки". 2020. № 2, Т 7.

2. Требін М. П. Феномен інформаційної війни у світі, що глобалізується: Вісник Національної юридичної академії України імені Ярослава Мудрого. Сер. : Філософія, філософія права, політологія, соціологія. 2013. № 2. С. 188–198.

3. Радковець Ю. І. Ознаки технологій «гібридної війни» в агресивних діях Росії проти України: Наука і оборона. 2014. № 3. С. 36–42.

4. Горбулін В. П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. Стратегічні пріоритети : Національний інститут стратегічних досліджень. 2014. № 4 (33). С. 5–10.

5. Б. В. Довгань , О. В. Мартинюк Становлення та розвиток поняття інформаційної війни: Вісник студентського наукового товариства Донецького Національного університету імені Василя Стуса. 2020. Вип.12. С. 51-56.

УДК 316.346.2

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ВЕБ-САЙТІВ НА ОСНОВІ МОДЕЛЕЙ РОЗПОДІЛЕННЯ ДОСТУПУ ТА МОНІТОРИНГУ ІДЕНТИФІКАТОРІВ КОРИСТУВАЧА

Беспалько Олександр, Ткачук Ростислав, Андріїв Роман
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. Кількість організацій, які використовують веб-технології для підвищення продуктивності та залучення нових клієнтів, зростає з кожним роком. Серед них - державні та місцеві органи влади, а також комерційні підприємства різних форм власності. Без сумніву, онлайн-сервіси пропонують багато переваг, але є дві сторони медалі. Зі збільшенням кількості додатків зростає і кількість кіберзагроз. Дослідження також фокусується на інтеграції нових методів безпеки в існуючі інфраструктури веб-сайтів та аналізує їх сумісність з іншими системами безпеки. В результаті можуть бути розроблені практичні рекомендації та інструменти для покращення кібербезпеки веб-сайтів.

Ключові слова: кібербезпека, веб-сайти, захист.

Abstracts. The number of organizations using web technologies to increase productivity and attract new customers is growing every year. Among them are state and local authorities, as well as commercial enterprises of various forms of ownership. There is no doubt that online services offer many benefits, but there are two sides to the coin. As the number of applications increases, so does the number of cyber threats. The study also focuses on the integration of new security methods into existing website infrastructures and analyzes their compatibility with other security systems. As a result, practical recommendations and tools can be developed to improve website cybersecurity.

Keywords. cybersecurity, websites, protection.

Захист веб-сайтів залишається одним з найважливіших напрямків інформаційної безпеки. З кожним роком збільшується кількість веб-сайтів, а також обсяг чутливої інформації, локалізованої на серверах віддаленого доступу особливо з використанням хмарних технологій. Як наслідок, зростає не лише кількість атак на веб-сайтів, але й економічні наслідки таких атак. Останнім часом вразливість веб-сайтів до атак набула політичного виміру у зв'язку з поширенням гібридних війн. Таким чином, вдосконалення методів і систем захисту веб-сайтів від атак залишається актуальним науковим завданням, особливо з огляду на постійне вдосконалення методів і засобів атак та появу нових методів і засобів. Удосконалення методів захисту веб-сайтів від атак є також важливим завданням і в практичному застосуванні через зростання економічних, соціальних і політичних наслідків зловмисних дій.

Стратегія тестування, яка використовується для вивчення захищеності системи та аналізу ризиків, пов'язаних із загальним підходом до захисту додатків, хакерських атак, вірусів і несанкціонованого доступу до конфіденційних даних. Тестування спрямоване на діагностику методів злому системи, оцінку захищеності веб-застосунків і веб-сайтів та аналіз ризиків, пов'язаних із підходом до захисту від зловмисників і доступу до конфіденційних даних. Тестування безпеки, засноване на принципах конфіденційності, доступності та цілісності, дає змогу забезпечити безпеку даних, облікових записів, доступу користувачів і з'єднань.

Загальна стратегія безпеки базується на трьох ключових принципах: конфіденційність, цілісність і доступність. Конфіденційність означає приховування певних ресурсів або інформації. Конфіденційність можна розуміти як обмеження доступу до ресурсу певної категорії користувачів, іншими словами, обмеження того, за яких умов користувачеві дозволено доступ до цього ресурсу.

Існує три підходи до виявлення вразливостей веб-додатків: тестування "чорного ящика", тестування "сірого ящика" та тестування "білого ящика". Різниця між ними залежить від ресурсів, доступних під час тестування [1].

Перший тип, тестування білого ящика, дає доступ до всіх ресурсів, включаючи вихідний код, технічні специфікації та всі види документації.

Другий тип, так зване тестування "чорного ящика", не вимагає знання внутрішньої структури програми, а лише вміння взаємодіяти з нею. Прикладом такого типу тестування є зовнішній аудит веб-додатків із закритим кодом.

Третій тип, тестування в "сірий ящик", означає, що в розпорядженні експертів є виконуваний файл і, можливо, деяка базова документація.

Загалом близько 300 веб-додатків з них для поглибленого аналізу було обрано 40 систем з найповнішим охопленням сканування. До статистики включено дані лише із зовнішніх веб-додатків, доступних з глобальної мережі Інтернет.

Досліджувані веб-додатки належать компаніям, що представляють різні галузі, включаючи електронну комерцію (30%), фінанси і банківську справу (22%), промисловість (17%), інформаційні технології (15%) і телекомунікації (13%), а також одну державну організацію, яка також брала участь у дослідженні. Більшість веб-додатків у вибірці були розроблені на основі PHP (58%) та ASP.NET (25%). Усі 40 досліджених веб-додатків мали ті чи інші вразливості, загалом 1194 вразливості. При цьому 68% систем містили вразливості з високим рівнем ризику. Більшість виявлених вразливостей 89% були спричинені помилками в програмному коді, і лише 11% недоліків були пов'язані з неправильним налаштуванням веб-додатків [2].

Банківська галузь очолила список за кількістю систем з уразливостями високого ризику 89%. Критичні уразливості були виявлені на 71% продуктивних веб-ресурсів у порівнянні з 50% тестових сайтів.

В ході дослідження безпеки фахівців Positive Technologies, ми порівняли результати тестування "білого ящика" (з використанням внутрішніх даних системи, включаючи аналіз вихідного коду) з результатами тестування "чорного ящика" і "сірого ящика" (аналіз проводився з тими ж привілеями, що і у потенційних зловмисників). Результати дослідження виявилися такими, що частка сайтів, що містять уразливості високого та середнього рівня ризику, була майже однаковою для цих методів тестування, то відсутність доступу до вихідного коду не робить веб-додаток безпечним.

Інформаційні веб-ресурси також піддаються різноманітним загрозам, і ефективна модель розподілу доступу грає важливу роль у їхньому захисті. Наведемо загрози, на які можуть наражатися веб-ресурси, та основні аспекти їхнього захисту [1, 3]:

- SQL-ін'єкції – атаки, спрямовані на впровадження шкідливого SQL-коду через веб-форми або інші вхідні дані. Ці атаки можуть призвести до видалення, модифікації або заміни даних у базі даних.
- Атаки на сесії – перехоплення сесій або використання крадених кредитів для несанкціонованого входу. Важливо використовувати безпеку сесій та механізми множинного фактора аутентифікації.
- Cross-Site Scripting (XSS) – атаки, при яких впроваджується зловмисний скрипт в веб-сторінку, який потім виконується на браузері користувача. Це може призвести до крадіжки інформації або видачі змісту зловмиснику.
- Cross-Site Request Forgery (CSRF) – атаки, при яких атакувальник використовує автентифіковану сесію користувача для виконання несанкціонованих дій в системі в їхньому ім'я.
- Brute Force атаки – спроби намагань атакувальника вгадати паролі, використовуючи повноцінні словники або інші методи.
- Витіснення файлів – спроби атакувальників отримати доступ до файлів або інформації, до яких вони не повинні мати доступ.
- Несанкціонований доступ до бази даних - атаки на рівень бази даних, які можуть викликати витік конфіденційної інформації або навіть видалення даних.
- Неатентна обробка помилок – виведення деталей помилок або витіснення конфіденційної інформації через помилки в програмному забезпеченні.
- Атаки на веб-фаєри – спроби використовувати вразливості веб-фаєрів для отримання несанкціонованого доступу або введення зловмисного коду.

- Недостатній контроль доступу – відсутність або недостатньо ефективний механізм контролю доступу, який призводить до несанкціонованого доступу до ресурсів.

Моделі розподілення доступу, такі як RBAC або ABAC, можуть допомагати в управлінні правами доступу та зменшенні ризиків внаслідок вказаних атак. Однак важливо постійно вдосконалювати системи безпеки, враховуючи нові загрози та вразливості.

Класичним пристроєм для захисту від веб-атак є брандмауер веб-додатків. Брандмауер веб-додатків застосовує набір правил безпеки до високорівневих протоколів додатків, таких як HTTP/HTTPS і FTP/FTPS. Під час встановлення WAF у мережі його розміщують перед веб-сервером, що захищається. Зазвичай його встановлюють у режимі зворотного проксі.

Набір функцій WAF зазвичай охоплює такі типові механізми захисту: перевірку протоколів; аналіз сигнатур; захист сесій і cookie; блокування витоку даних; виявлення атак (негативні моделі, атаки додатків, мережі та ОС); атаки на веб-сервер і ОС; можливість створення власних правил захисту, машинне навчання.

Моніторинг ідентифікації користувача є важливою складовою сучасних систем безпеки та управління доступом. Цей процес включає в себе систематичне спостереження за вхідними та вихідними інформаційними потоками для впевненості в правомірності дій конкретного користувача. Для досягнення цієї мети використовуються різноманітні технології, такі як біометричні сканери, аналіз поведінки користувача, та методи аутентифікації на основі апаратних ключів. Моніторинг ідентифікації користувача є невід'ємною частиною систем безпеки в інформаційному середовищі та відіграє ключову роль у попередженні несанкціонованого доступу до конфіденційної інформації та ресурсів.

Література

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

2. Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2011. – Вип. 2 (92). – С.53-56.

3. Jones, M., & Brown, A. "Behavioral Biometrics in User Authentication: A Survey." International Journal of Information Security, – 2020. – Вип. 25(4). – С.567-589.

УДК 004.77

ІНСТРУМЕНТИ МОНІТОРИНГУ МЕРЕЖЕВИХ З'ЄДНАНЬ

Біленко Ярослав, Фединець Наталія
Львівський державний університет безпеки життєдіяльності, Львів

Анотація: Сучасний світ безперервно піддається трансформаціям завдяки стрімкому розвитку технологій мережевого зв'язку. Міжмережеві з'єднання стали критично важливою складовою для підтримки комунікаційних інфраструктур, що обслуговують різноманітні сфери, включаючи бізнес, науку, медицину та соціальні послуги. Для забезпечення надійності та безпеки цих мереж необхідно розробляти та використовувати інструменти моніторингу міжмережевих з'єднань.

Ключові слова: моніторинг міжмережевих з'єднань, надійність мережі, безпека мережі, інструменти моніторингу, мережевий трафік, вразливості мережі.

Abstract: The modern world is constantly undergoing transformations due to the rapid development of network communication technologies. Interconnections have become a critical component in supporting communication infrastructures serving a variety of fields, including business, science, medicine, and social services. To ensure the reliability and security of these networks, it is necessary to develop and use tools for monitoring interconnections.

Keywords: monitoring of network connections, network reliability, network security, monitoring tools, network traffic, network vulnerabilities.

Забезпечення надійності мережевих з'єднань є першочерговим завданням для компаній, урядових структур та організацій у сучасному інформаційному віці. Негативні наслідки можуть бути надто серйозними, якщо мережеві з'єднання не функціонують належним чином. Від дрібних відключень до масштабних кібератак, загрози для мережевої надійності можуть мати катастрофічні наслідки.

Однією з ключових функцій моніторингу міжмережевих з'єднань є забезпечення безпеки мережі. Інструменти моніторингу дозволяють виявляти та відповідати на потенційні загрози для інформаційної безпеки, включаючи вразливості, несанкціонований доступ, атаки з метою видалення даних та інші аномалії [1, 2].

Моніторинг також допомагає підвищити реактивність інфраструктури щодо виявлення та відвертання атак. Швидке виявлення та відповідь на загрози стають рішучими у боротьбі з сучасними кіберзлочинністю та кібершпіонажем.

Моніторинг міжмережевих з'єднань допомагає ефективно розподіляти ресурси мережі. Аналізується використання мережевого обладнання, яке дозволяє планувати їхню модернізацію та оптимізувати пропускну здатність.

Моніторинг ресурсів допомагає визначати перевантажені ділянки мережі та вчасно вживати заходи для забезпечення належного рівня обслуговування для користувачів. Це особливо важливо в умовах зростаючого обсягу мережевого трафіку та розширення послуг, пропонованих через мережу.

Моніторинг мережевого трафіку є ключовим елементом для покращення якості обслуговування користувачів. Аналіз трафіку допомагає ідентифікувати структуру та властивості трафіку, а також виявляти проблеми, що можуть виникати під час передачі даних. Це важливо для забезпечення належної якості послуг у вимогливих застосуваннях, таких як стрімінг відео, онлайн-ігри та віртуальні конференції [3].

У сучасний епоху доступний широкий спектр інструментів моніторингу, які надають можливості для ретельного аналізу мережевого стану. До них відносяться:

1. Системи ведення журналів: Ці системи забезпечують збір і аналіз логів подій для виявлення аномалій та небезпек.
2. Системи моніторингу ресурсів: Вони надають інформацію про використання процесора, пам'яті, дискового простору та інших ресурсів, що допомагає планувати їхню оптимізацію.
3. Системи аналізу мережевого трафіку: Ці інструменти дозволяють детально вивчати пакети трафіку, виявляти аномалії та оптимізовувати роботу мережі.
4. Системи виявлення загроз: Вони спрямовані на виявлення потенційно шкідливих активностей в мережі, включаючи віруси, шкідливі програми та злочинні атаки.

Моніторинг міжмережевих з'єднань відіграє вирішальну роль у забезпеченні надійності, безпеки та ефективності мережевих інфраструктур. Сучасні інструменти моніторингу дозволяють виявляти та вирішувати проблеми швидше і ефективніше, що сприяє покращенню якості обслуговування та підвищенню безпеки мереж зв'язку. Розробка та впровадження таких інструментів стають стратегічно важливими завданнями для організацій у світі інформаційних технологій, де надійність і безпека мереж стають ключовими факторами успіху.

Література

1. Сивобородько А.В., Говоруха В. І. Аспекти застосування технічних засобів моніторингу та фільтрації сигнального трафіку як один із напрямів підвищення безпеки електронних комунікаційних мереж. The 3 rd International scientific and practical conference “Modern problems of science, education and society”(May 22-24, 2023) SPC “Sci-conf. com. ua”, Kyiv, Ukraine. 2023. 1522 p.
2. Жилін А.В., Шаповал О.М., Успенський О.А. Технології захисту інформації в інформаційно-телекомунікаційних системах. 2020.
3. Глазок О.М. Моніторинг мережевої активності комп'ютерів на основі агентної технології. 2012.

УДК 004.77

ТАКТИКА МОДЕЛЕЙ CYBER KILL CHAIN І UNIFIED KILL CHAIN: РОЗКРИТТЯ АНАТОМІЇ КІБЕРАТАК

Боднар Остап, Ткачук Ростислав
Львівський державний університет безпеки життєдіяльності, Львів

Анотація: Ця стаття розглядає концепцію ланцюгів Cyber Kill Chain та Unified Kill Chain, які є стратегічним підходом до аналізу та протистояння кібератакам. Ці ланцюги, визначають етапи кібернападу від початкового етапу розвідки до завершення атаки. Проведено дослідження кожного з етапів цих ланцюгів, розкриваються характеристики та методики, які зловмисники використовують на кожному етапі.
Ключові слова: Кіберланцюг, кібербезпека, кібератаки, кіберзагрози, вторгнення, експлуатація.

Abstract: This article discusses the concepts of Cyber Kill Chain and Unified Kill Chain, which are a strategic approach to analyzing and countering cyber attacks. These chains define the stages of a cyber attack from the initial stage of reconnaissance to the completion of the attack. The author studies each of the stages of these chains, reveals the characteristics and techniques used by attackers at each stage.
Keywords: Cyber chain, cybersecurity, cyber attacks, cyber threats, intrusion, exploitation.

Кіберзагрози часто змінюються, як і тактика захисту та запобігання. Сьогодні все більше організацій реалізують багаторівневий підхід до кібербезпеки, який охоплює адміністративний, технічний і фізичний контроль безпеки. Однак навіть із застосуванням найсучасніших технічних засобів захисту деякі організації неминуче стають жертвами успішних кібератак.

Для ефективної боротьби з цими загрозами були розроблений широкий спектр практик, інструкцій, політик та моделей кібербезпеки. Одним із таких фреймворків, який набув популярності, є Cyber Kill Chain. Cyber Kill Chain, розроблений оборонним підрядником Lockheed Martin у 2011 році, забезпечує структурований підхід до розуміння та протидії кіберзагрозам, який реалізується шляхом виявлення та припинення зловмисної діяльності. Термін Cyber Kill Chain – це військова концепція, пов'язана зі структурою атаки. Він працює за чітким агоритмом: ідентифікації цілі, рішення і наказу атакувати ціль і, нарешті, знищення цілі. Ця система визначає кроки, які використовують супротивники або зловмисники в кіберпросторі. Щоб досягти успіху, супротивник повинен пройти через усі фази так званого "ланцюга вбивства" [1].

Здебільшого організації використовують ланцюжок кіберзагроз для захисту від найскладніших кібератак, зокрема програм-вимагачів, порушень безпеки та вдосконалених постійних загроз (APT).

Cyber Kill Chain допоможе зрозуміти та захиститися від атак з вимогою викупу, порушень безпеки, а також від сучасних постійних загроз. Cyber Kill

Chain можна використовувати для оцінки безпеки приватної мережі та системи, визначаючи відсутні засоби контролю безпеки та закриваючи певні прогалини у безпеці, виходячи з інфраструктури компанії [2].

Розуміючи ланцюжок кібератак як SOC-аналітик, дослідник безпеки, мисливець за загрозами або фахівець з реагування на інциденти, можна розпізнавати спроби вторгнення і розуміти цілі та завдання зловмисника.

Cyber Kill Chain включає наступні етапи атаки (рис. 1) [2, 3, 5]:

- розвідка;
- озброєння;
- доставка;
- експлуатація;
- встановлення;
- командування та управління;
- дії по досягненню цілей.

Перший етап «Розвідка». Розвідка включає в себе виявлення та збір інформації щодо системи та потенційної жертви, і вважається етапом планування для атак. Зловмиснику необхідно детально вивчити об'єкт нападу, збираючи доступні дані про компанію та її працівників з відкритих джерел. Ця інформація включає розмір компанії, електронні адреси, телефонні номери тощо, з метою визначення оптимальної цілі для атаки.

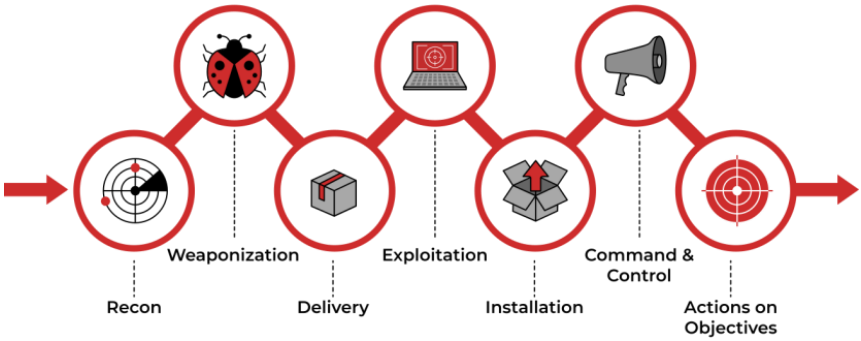


Рисунок 1 – Етапи ланцюга Cyber Kill Chain

Другий етап «Озброєння». Після успішного етапу розвідки зловмисник працюватиме над створенням "зброї знищення". Він вважатиме за краще не взаємодіяти з жертвою безпосередньо, а замість цього створить "зброєносець", який, за словами Lockheed Martin, об'єднує шкідливе програмне забезпечення і експлойт в корисне навантаження, що доставляється.

Третій етап «Доставка». Фаза доставки – це коли зловмисник вирішує вибрати метод передачі корисного вантажу або шкідливого програмного забезпечення, де він може бути виконаний на системі жертви. У нього є безліч варіантів на вибір:

- фішинговий електронний лист;
- розповсюдження заражених USB-накопичувачів у громадських місцях;
- атака на водопій.

Четвертий етап «Експлуатація». На етапі експлуатації відбувається фактична компрометація. Зловмисники використовують вразливості в цільовій системі або додатку, щоб запустити свій шкідливий код і закріпитися в мережі. Це може включати використання вразливостей програмного забезпечення, неправильних конфігурацій або людського фактору. На етапі експлуатації зловмисники часто намагаються досягти певної мети, наприклад, отримати несанкціонований доступ, підвищити привілеї або закріпитися в цільовому середовищі.

П'ятий етап «Встановлення (Стійкість)». Після того, як зловмисник отримав доступ до системи, він захоче знову отримати доступ до системи, якщо втратить зв'язок з нею, або якщо його виявлять і позбавлять початкового доступу, або якщо систему пізніше буде виправлено. Він більше не матиме до неї доступу. Саме тоді зловмиснику необхідно встановити бекдор. Стійкий бекдор дозволить зловмиснику отримати доступ до системи, яку він скомпрометував у минулому.

Шостий етап «Командування та контроль». Після отримання стійкості та виконання шкідливого програмного забезпечення на комп'ютері жертви, зловмисник відкриває канал C2 через шкідливе програмне забезпечення для віддаленого управління та маніпулювання жертвою. Скомпрометована кінцева точка зв'язується із зовнішнім сервером, встановленим зловмисником для створення каналу управління. Після встановлення з'єднання зловмисник отримує повний контроль над комп'ютером жертви.

Сьомий етап «Дії по досягненню цілей». Пройшовши через шість фаз атаки, зловмисник може нарешті досягти своїх цілей. "Дії по досягненню цілей" зосереджуються на кінцевій меті зловмисника, яка може змінюватися залежно від характеру атаки. Цей етап передбачає виконання конкретних зловмисних дій або досягнення поставлених цілей, які спонукали до кібератаки в першу чергу. Це можуть бути такі дії, як викрадення даних, виведення системи з ладу, шпигунство або будь-яка інша мета, яку прагне досягти зловмисник.

Але незважаючи на те, що оригінальна модель кіберланцюжка вбивства містить лише сім етапів, експерти з кібербезпеки розширили ланцюжок вбивства, включивши восьмий етап – монетизацію.

Восьмий етап «Монетизація». На етапі монетизації зловмисники зосереджуються на отриманні прибутку від успішної атаки, чи то через певну форму викупу, чи то через продаж конфіденційної інформації в темній мережі.

З моменту створення ланцюжок кіберзагроз еволюціонував, щоб краще передбачати та розуміти сучасні кіберзагрози. Його також прийняли організації та фахівці з безпеки даних, щоб допомогти визначити етапи атаки.

Проте не існує в сфері кіберзахисту універсального підходу, так званої «срібної кулі» і модель кібербезпеки Cyber Kill Chain теж не є виключенням. Існують і певні слабкі місця у цій моделі їх можна звести до основних двох категорій: безпека периметра та вразливості до атак [4].

Охорона периметра. Однією з найбільших критики моделі Cyber Kill Chain від Lockheed є той факт, що перші дві фази атаки (розвідка та створення зброї) часто відбуваються за межами цільової мережі. Це може ускладнити для організацій розуміння або захист від будь-яких дій, що відбуваються на цих етапах.

І друга ***вразливості до атак*** деякі дослідження показують що метод може підсилювати традиційні захисні стратегії на основі периметра та запобігання зловмисному програмному забезпеченню, яких недостатньо в сучасному просторі кібербезпеки.

Крім того, деякі критики вважають, що традиційний кіберланцюжок знищення не є придатною моделлю для імітації внутрішніх загроз. Це потенційно піддає організації більшому ризику, враховуючи ймовірність успішних атак, які порушують периметр внутрішньої мережі цільової мережі.

Дані недоліки може компенсувати уніфікована модель Kill Chain. Unified Kill Chain була розроблена у 2017 році Полом Полсом у співпраці з Fox-IT і Лейденським університетом, щоб подолати загальну критику традиційного кіберланцюга вбивств. Ця модель об'єднала та розширила фреймворк Lockheed's Kill Chain та фреймворк MITRE ATT&CK.

Уніфікована модель ланцюга знищення була розроблена для захисту від наскрізних кібератак з боку різноманітних досвідчених зловмисників і надає розуміння тактики, яку використовують хакери для досягнення своїх стратегічних цілей (рис. 2).

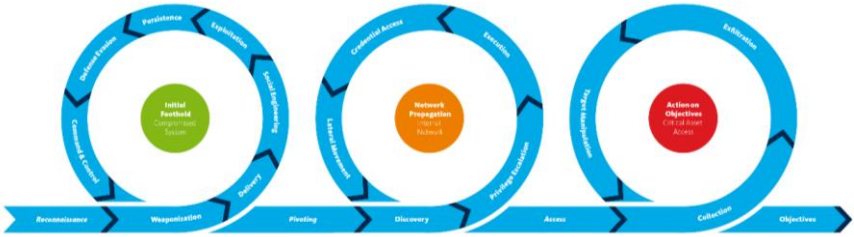


Рисунок 2 – Етапи ланцюга Unified Kill Chain

Ця модель розбита на три основні фази: початкова точка опори, поширення мережі та дія щодо цілей.

Кожна з цих фаз складається з додаткових фаз атаки. Загалом існує 18 фаз [4].

Розвідка: дослідження, ідентифікація та вибір цілей шляхом активного або пасивного спостереження.

Озброєння: методи підготовки, спрямовані на створення необхідної інфраструктури для нападу.

Доставка: методи, які допомагають у передачі озброєного об'єкта в цільове середовище.

Соціальна інженерія: методи, спрямовані на маніпулювання людьми для виконання небезпечних дій.

Експлуатація: тактика використання вразливостей системи, яка може призвести до виконання коду.

Постійність: будь-яка дія, доступ або зміна системи, які надають зловмиснику постійну присутність у системі.

Ухилення від захисту: тактика ухилення, яку зловмисник може використовувати спеціально для того, щоб уникнути виявлення чи інших засобів захисту.

Командування та контроль: методи, які дозволяють зловмисникам спілкуватися з контрольованими системами в цільовій мережі.

Обертання: використання контрольованої системи для тунелювання трафіку до інших систем, до яких немає прямого доступу.

Виявлення: методи, які дозволяють зловмиснику отримати інформацію про систему та її мережеве середовище.

Підвищення привілеїв: результат прийомів, які надають зловмиснику вищі дозволи в системі чи мережі.

Виконання: тактика, яка призводить до виконання контрольованого зловмисником коду на локальній або віддаленій системі.

Доступ до облікових даних: стратегії, які забезпечують доступ або контроль над обліковими даними системи, служби чи домену.

Латеральний рух: методи, які використовуються для розширення охоплення атаки та пошуку нових систем або даних, які можуть бути скомпрометовані.

Збір: методи ідентифікації та збору даних із цільової мережі перед викраденням.

Викрадання: тактика, яка допомагає або призводить до видалення зловмисником даних із цільової мережі.

Вплив: методи маніпулювання, переривання або знищення цільової системи чи даних.

Цілі: Соціально-технічні завдання атаки, спрямовані на досягнення стратегічної мети.

Отже незважаючи на те, що ланцюжок кіберубивств надзвичайно цінний, це лише структура. Організаціям важливо мати відповідне програмне забезпечення для кібербезпеки, щоб забезпечити необхідні можливості запобігання та виявлення.

Наприклад, інструменти розширеного виявлення та реагування (XDR) стають все більш важливими для успіху сучасних стратегій кібербезпеки. XDR, який іноді називають «міжрівневим» або «будь-яким джерелом даних», виявлення та відповідь, виходить за межі кінцевої точки,

щоб приймати рішення на основі даних з більшої кількості джерел і вживає заходів на різних платформах, діючи на електронну пошту, мережу, ідентифікаційні дані тощо.

За допомогою SentinelOne організації можуть запобігати, виявляти та перехоплювати як відомі, так і невідомі загрози, перш ніж вони завдадуть шкоди. Завдяки уніфікації та розширенню можливостей виявлення та реагування на кілька рівнів безпеки користувачі отримують найкращий у галузі захист у кожній сфері на одній платформі.

Організаціям більше не потрібно покладатися виключно на застарілий підхід, який перевіряє кібератаки постфактум. Натомість вони можуть впевнено випереджати загрози.

Література

1. Tarun Yadav(B) and Arvind Mallari Rao, (2015). Technical Aspects of Cyber Kill Chain. 439. DOI: 10.1007/978-3-319-22915-7_40

2. CyberKillChain Lockheed Martin [Електронний ресурс]. – Доступний з https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

3. Understanding the Cyber Kill Chain framework [Електронний ресурс]. – Доступний з https://subscription.packtpub.com/book/security/9781801818933/2/ch02lvl1sec09/understanding-the-cyber-kill-chain-framework

4. What Is The Cyber Kill Chain? Steps, Examples, & How To Use It [Електронний ресурс]. – Доступний з https://www.sentinelone.com/cybersecurity-101/cyber-kill-chain/

5. Організація захисту сайту створеного за технологіями: MONGODB, ANGULAR 12, HTML5, CSS3, JAVASCRIPT, NESTJS. Мельцов В. В., Ткачук Р. Л. VIII Всеукраїнська заочна науково – практична конференція “Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М. П. Драгоманова, 2022. С. 84–85.

УДК 004.42.58

ДОСЛІДЖЕННЯ МЕТОДІВ ПОКРАЩЕННЯ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ В СМАРТФОНІ ДЛЯ РЕАЛЬНИХ УМОВ

Боярчук Максим, Горпенюк Андрій
Національний університет "Львівська політехніка"

Описано методику захисту смартфону від розблокування на основі біометрики за відбитком пальця для реальних умов використання пристрою. Додаток реалізований мовою Kotlin. Проведено серію експериментів з додатком, врахування результатів яких дозволило покращити його роботу шляхом додаткового фактору (пін-коду).

Ключові слова: біометрика, смартфон, відбиток пальця, пін-код
Keywords: biometrics, smartphone, fingerprint, pin code

На сьогоднішній час смартфони потребують надійного захисту даних, які в них зберігаються. До таких даних можна віднести хеші паролів доступу до різноманітних сайтів, телефонну книгу, адреси електронної пошти, особисті фото, історію пошуку в Інтернеті. Фактично, якщо до рук злочинця потрапить смартфон з розблокованим доступом, він може розсилати електронні листи від імені власника, зробити крадіжку особистості, скористатись фінансовими інструментами власника, опублікувати в мережі приватні фото з метою компрометації та багато іншого. Тому дослідження із надійного блокування/розблокування мобільних пристроїв є затребуваними. Є достатньо велика кількість методів, які дозволяють власнику розблокувати смартфон, наприклад, ввести пін-код, накреслити на екрані геометричну фігуру, скористатись власною біометрикою [1]. В даному дослідженні розглянуто мультифакторну автентифікацію, в якості першого фактору використано відбиток пальця, в якості другого - пін код, оскільки це надає більшої безпеки у випадку викрадення злочинцем телефону. Для власника смартфону це дає можливість його розблокування у випадку помилкового спрацювання сканера відбитку.

Метою дослідження є створення додатку, який виконує розблокування екрану смартфону на основі роботи сканера відбитку пальця із декількома етапами автентифікації для забезпечення кращого захисту мобільного пристрою та можливості розблокування у випадку хибного спрацювання сканеру.

У роботі запропоновано вирішення цієї задачі шляхом застосування додатку біометричної автентифікації із мультифакторним входом, який після декількох невдалих спроб замість використання автентифікації за відбитком пальця додатково пропонує пройти автентифікацію за паролем (пін-кодом). На рис.1 наведено приклад додатку.

Для реалізації було використано Android Studio, і обрано мову написання Kotlin, так як вона пристосована для розробки андроїд додатків. В результаті було проведено дослідження, яке змогло показати, наскільки може бути затребуваний такий спосіб у повсякденному житті для реальних умов, коли розблокувати телефон потрібно не тільки в офісі чи вдома, а і для несприятливих для сканування умовах. Під несприятливими приймались таки умови, коли порушена позиція пальця при скануванні (це частіше може відбутись на вулиці чи в транспорті), або палець знаходиться в інших по відношенню до еталонного сканування умовах (наприклад, палець вологій, забруднений, або безпосередньо після фізичного напруження).

Досліди проводились на смартфоні Redmi Note 8 Pro в різні часи доби та для різних умов сканування. Було виконано декілька серій по 15 спроб у кожній серії. Зранку вдома через додаток було зроблено 15 спроб, результат був успішним у всіх спробах. Коли вдень руки деякий час були у теплій воді і були дещо вологими при скануванні, із 15 спроб позитивний результат був лише 2 рази. Днем на вулиці і в автобусі при холодній погоді під час сканування із 15 спроб були успішними 11 спроб.

Рисунок 1 – Сканер відбитку пальця

Аналогічні випробування було проведено для іншої особи, яка не була власником смартфону (шаблону її відбитку пальця не було в пам’яті додатку). Всі спроби були неуспішними. Результати розрахунку відсотку успішних спроб, а також FRR та FAR подані у табл. 1.

Таблиця 1 – Результати розпізнавання відбитку пальця власника в залежності від умов сканування

Умови сканування	Відсоток успішних спроб для власника, %	Відсоток неуспішних спроб для власника (FRR), %	Відсоток успішних спроб для іншої особи (FAR), %
Умови офісу, домівки, сухій палець	100,0	0,0	0,0
Умови офісу, домівки, вологій палець	13,(3)	86,(6)	0,0
Умови транспорту, на вулиці	73,(3)	26,(6)	0,0

Результати експерименту довели: сканер налаштований таким чином, що надійно запобігає розблокуванню смартфону сторонньою особою, але може створювати проблеми для власника. Тому в код додатку було додано можливість введення такого фактору автентифікації, як пін-код. При налаштуванні додатку передбачена можливість вибору кількості хибних спрацювань, після чого пропонується ввести пін-код. Таким чином, розроблений додаток пристосований під реальні умови використання біометрики для захисту смартфону.

Література

1. Cappelli, R. SFinGe. In *Encyclopedia of Biometrics*; Li, S.Z., Jain, A., Eds.; Springer: Boston, MA, USA, 2009; pp. 1169–1176.

УДК 004.738.5

ІНФОРМАЦІЙНА ВІЙНА

Будник Дарина, Дам-Васильєва Чанг Анжеліка
Харківський національний університет радіоелектроніки, м. Харків, Україна

Швидкий розвиток інформаційно-комунікаційних технологій визначає становище країни в глобальній економіці та політичний вплив. Прагнення до інформаційного домінування в геополітичній конкуренції створює загрози інформаційній безпеці, переростаючи в серйозні інформаційні конфлікти.

Ключові слова: війна, інформаційна війна, інформаційна безпека, фейки, інформація, суспільство.

The swift progress of information and communication technologies defines a nation's standing in the global economy and political influence. The quest for information dominance in geopolitical competition poses threats to information security, escalating into serious information conflicts.

Keywords: war, information war, information security, fakes, information, society.

Інформаційна війна - це форма зіткнення між різними суб'єктами, такими як держави, неурядові організації, економічні структури тощо. Вона включає в себе комплекс заходів для завдання шкоди інформаційній сфері противника та захисту власної інформаційної безпеки [1].

Історичний контекст появи терміну «інформаційна війна» пов'язаний із серединою 1980-х років, коли Сполучені Штати Америки ставали перед новими завданнями після завершення холодної війни.

Основна мета інформаційної війни між державами полягає в тому, щоб негативно впливати на політичну силу держави, а також у підриві міжнародних зв'язків та ослабленні політичного іміджу, включаючи ослаблення правлячої еліти, існуючого соціально-політичного режиму або навіть сприяння їх відстороненню від влади.

Основний об'єкт такої війни - це громадська думка та свідомість окремих осіб. Об'єкти, які піддаються впливу в межах цієї війни, можуть бути загальними, спеціальними або відноситися до розвідувальних спрямувань [2].

Інститут національно-стратегічних досліджень США та західні експерти зі вченими виділяють наступні аспекти інформаційної війни:

1. Стратегія і тактика нейтралізації командної структури противника.
2. Розвідувальна війна, яка включає в себе збір і аналіз розвідувальної інформації.
3. Електронна війна, спрямована на вплив на електронні системи та комунікації.

4. Психологічна війна, спрямована на вплив на свідомість та психологічний стан населення та військових.

5. Комп'ютерна війна, яка включає в себе атаки та оборону в комп'ютерних мережах та системах.

6. Інформаційна війна в економічній сфері, яка включає в себе атаки на економічні системи та структури.

7. Інформаційний тероризм, спрямований на створення паніки та хаосу шляхом поширення дезінформації та використання інших терористичних методів [3].

Переможцем в інформаційній війні стає та сторона, яка краще вміє прогнозувати та моделювати поведінку свого супротивника в різних ситуаціях, розробляти власні стратегії та впливати на суспільну думку. Для досягнення успіху необхідно збирати, аналізувати та зберігати велику кількість інформації про супротивника, розуміти його культуру, історію, релігію та інші аспекти.

Як приклад можна вказати інформаційну війну, яку російська федерація веде проти України протягом останніх 10-15 років. Особливо гострого характеру вона набула з 2014 - від часу переходу рф до гібридної війни проти України, яка супроводжувалася російською анексією Криму і визнанням рф незаконних квазідержавних утворень в особі так званих Донецької та Луганської народних республік.. Новий поштовх потужного інформаційного протистояння між росією і Україною був викликаний повномасштабною війною, яку рф розв’язала 24.02.2022 проти України [4].

Напрямами та способами інформаційних війн росії проти України були й залишаються: поступове зниження міжнародного іміджу України з метою послаблення її геополітичного значення; відповідне дозування та спотворення інформації з метою дестабілізації ситуації в державі та впровадження власної політики «керованого хаосу»; формування стереотипу меншовартості та вторинності українців, а також відповідне руйнування почуття нації та народу; домінування російської мови, культури та традицій для утвердження самоідентифікації при одночасному витісненні української мови та культури.

Російська федерація використовує такі методи інформаційної війни: «дозована інформація»; дезінформація у поєднанні із великим викривленням подій; подача припущень, особистих думок та вибіркові, корисні для пропагандиста, факти; інформаційний рефреймінг; перекручування інформації і її подача «без коментарів»; технологія «25-го кадру», яка заборонена міжнародним законодавством; замовчування важливих подій.

Виконання вказаних завдань було здійснено за допомогою широкого спектру комунікаційних каналів, зокрема:

1. Засоби масової інформації (ЗМІ) в традиційному форматі.
2. Електронні ЗМІ, зокрема телебачення.
3. Інтернет-медіа.

4. Соціальні мережі [1].

На жаль, всі ці методи впливають на психіку людей та суспільства загалом. Тому важливо витрачати час на ретельну перевірку новин. Ось кілька порад, як це зробити ефективно:

1. Навчитися читати статті повністю перед тим, як виразити свою думку або поставити «лайк».

2. Використовувати різні доступні засоби для перевірки надійності видань.

3. Уважно дивитися на дату публікації, оскільки деякі матеріали можуть бути переосмислені чи повторно опубліковані з метою збільшення популярності.

4. Звертати увагу на джерела, які підтверджують представлені факти реальними даними.

5. Аналізувати цитати та фотографії, щоб визначити їхню достовірність.

6. Шукати інші видання для порівняння, особливо, якщо історія викликає сумніви.

Підсумовуючи, варто відзначити, що інформаційна війна росії проти України проводиться систематично та цілеспрямовано, призводячи до серйозних людських та матеріальних втрат серед населення і об'єктів. Ця інформаційна кампанія слугує прикриттям для російської агресії проти України, порушуючи міжнародне гуманітарне право. Використання збройних сил у Криму та підтримка терористів на Донбасі є явним порушенням міжнародного права, а використання інформаційної зброї сприяє розгортанню ксенофобії, тероризму і дискредитації українського уряду. Це свідчить не лише про проведення інформаційної війни, а й про її протиправність, порушення міжнародного правового порядку.

Література

1. ВікіпедіЯ. (2023, 20 листопада). Інформаційна війна. https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B2%D1%96%D0%B9%D0%BD%D0%B0

2. Українська правда. (2023, 20 листопада). Інформаційна війна – зброя масового знищення! https://www.pravda.com.ua/rus/articles/2006/04/20/4399050/

3. Політологія. (2023, 21 листопада). Поняття інформаційної війни. http://politics.ellib.org.ua/pages-8282.html

4. Велика Українська Енцеклопедія. (2023, 21 листопада). Інформаційна війна. https://vue.gov.ua/96%D0%B9%D0%BD%D0%B0

УДК 004.77

РОЛЬ ОПЕРАЦІЙНОЇ СИСИТЕМИ LINUX У КІБЕРБЕЗПЕЦІ

Букартик Олег, Ткачук Ростислав
Львівський державний університет безпеки життєдіяльності, Львів

Анотація: Операційна система Linux відіграє важливу роль у сфері кібербезпеки, забезпечуючи надійну та безпечну основу для розробки та впровадження заходів інформаційної безпеки. У цій статті описується різні аспекти використання Linux в кібербезпеці, починаючи з функцій безпеки операційної системи. Linux відрізняється від інших операційних систем своєю відкритістю і відкритими можливостями аудиту, що робить його популярним серед експертів в області безпеки. У цій праці також описується роль Linux у вирішенні завдання моніторинг.

Ключові слова: Кібербезпека, безпека операційної системи, відкритість, аудит, моніторинг, системи журналювання, виявлення вторгнень.

Abstract: Linux plays an important role in the field of cyber security, providing a reliable and secure foundation for the development and implementation of information security measures. This article describes various aspects of using Linux in cybersecurity, starting with the security features of the operating system. Linux differs from other operating systems in its openness and auditing capabilities, which makes it a popular security expert. This report also discusses the role of Linux in solving the task of monitoring.

Keywords: Cyber security, jperating system security, jpenness, audit, monitoring, logging systems, intrusion detection.

Поняття кібербезпеки має на увазі під собою сукупність методів, технологій і процесів, призначених для захисту цілісності мереж, програм і даних від цифрових атак. Метою кібератак є отримання несанкціонованого доступу до конфіденційної інформації, її копіювання, зміни або знищення. На шляху до мети зловмисника стоїть операційна система і від її надійної роботи залежить його успіх чи невдача.

Linux – це сімейство Unix-подібних операційних систем, що використовують ядро Linux, яке розробив Лінус Торвальдс. ОС, які використовують ядро Linux, називаються дистрибутивами Linux (рис. 1) [1].

Рисунок 1 – Пінгвін Tux – Талісманом Linux

Для підвищення продуктивності Linux, використовується традиційне монолітне ядро з елементами модульної архітектури (завдяки чому для більшості драйверів доступна можливість динамічно завантажувати та вивантажувати дані під час виконання).

Ядро Linux було написано в 1991 році (набагато пізніше, ніж була створена перша версія Windows) Лінусом Торвальдсом, який хотів створити вільне ядро ОС, яке зможе використати будь-хто. Сьогодні ядро Linux містить понад 23 мільйони рядків вихідного коду, яке поширюється (починаючи з 1992 року) під ліцензією вільного програмного забезпечення GNU General Public License [1].

Забезпечення безпеки системи

Linux відомий своєю стійкістю до атак і здатністю забезпечувати безпеку на рівні ядра завдяки відкритому коду, код може бути протестований та перевірений експертами з кібербезпеки для виявлення та усунення вразливостей. Важливими аспектами безпеки операційної системи Linux є використання SELinux (Security-Enhanced Linux) та AppArmor для захисту від атак, що включає в себе обмеження прав доступу до ресурсів. Тобто обмеження привілеїв та контроль доступу до ресурсів. Крім того, механізми контролю доступу, такі як аудит SELinux, допомагають відстежувати спроби несанкціонованого доступу та реагувати на них. Linux має високу стійкість до різних типів атак завдяки кільком важливим особливостям [2, 3, 5]:

1. *Відкритий вихідний код*. Загальна публічна ліцензія GNU надає доступ до вихідного коду Linux, що дозволяє експертам з кібербезпеки перевіряти код на наявність вразливостей. А також це робить можливим виявляти та виправляти потенційні проблеми безпеки.

2. *Механізми контролю доступу*. Linux використовує механізми контролю доступу, такі як SELinux (Security-Enhanced Linux) та AppArmor для обмеження привілеїв процесів. Це допомагає обмежити доступ шкідливого програмного забезпечення до критично важливих ресурсів і даних у системі.

3. *Політика безпеки на рівні ядра*. Ядро Linux було ретельно спроектовано з урахуванням безпеки, і розробники доклали чимало зусиль, щоб зробити його стійким до атак. Одним з ключових елементів є системні виклики, які обмежують доступ до ресурсів.

4. *Обов'язковий контроль доступу (MAC)*. SELinux та AppArmor використовують обов'язковий контроль доступу, щоб зробити систему ще більш безпечною. Він надає детальні політики доступу до ресурсів і файлів та допомагає запобігти атакам на систему.

5. *Регулярні оновлення та патчі*. Розробники Linux регулярно випускають оновлення та патчі для усунення виявлених вразливостей. Це гарантує, що система залишатиметься актуальною та безпечною. Забезпечення безпеки на рівні операційної системи є першим і фундаментальним кроком у кібербезпеці, тому Linux надає ефективні інструменти для досягнення цієї мети.

Моніторинг та аналіз подій

Одним з ключових аспектів кібербезпеки є здатність виявляти, відстежувати та реагувати на потенційно небезпечні події в системі. Linux надає набір інструментів для моніторингу та аналізу подій:

1. *Ведення журналів (syslog і journald)*. Linux має розвинену систему ведення журналів, яка може записувати події у системі.

2. *Інструменти для виявлення несанкціонованого доступу*. Додаткові інструменти, такі як Fail2ban, використовуються для виявлення та фільтрації спроб несанкціонованого доступу до системи. IP-адреси з надмірною кількістю спроб входу можуть бути заблоковані.

Fail2ban – це інструмент, який відстежує системні журнали на предмет надмірної кількості спроб несанкціонованого доступу, наприклад, спроб входу з неправильним паролем. Якщо кількість спроб перевищує певний ліміт, Fail2ban може заблокувати IP-адресу, з якої здійснюються спроби.

3. *Інструменти виявлення вразливостей*. Linux також підтримує ряд інструментів виявлення вразливостей, які допомагають виявити потенційні проблеми безпеки в системі.

Snort і Suricata – це системи виявлення мережевих вразливостей і вторгнень. Вони аналізують мережевий трафік і виявляють дії, які можуть вказувати на шкідливі пакети або мережеві атаки. Ці інструменти також можуть надсилати сповіщення про підозрілу активність і автоматично блокувати атаки.

4. *Антивірус та антивірусне програмне забезпечення*. Linux підтримує різноманітні антивірусні та антишпигунські програми, які можуть виявляти та нейтралізувати шкідливий код, який може загрожувати системі. Використовуючи ці інструменти, експерти з кібербезпеки можуть виявляти і реагувати на загрози, які можуть виникати в системах Linux. Цей аспект моніторингу та аналізу інцидентів відіграє важливу роль у кібербезпеці, оскільки дозволяє своєчасно виявляти та реагувати на потенційні загрози та атаки на систему.

Централізований моніторинг та аналіз

У великих середовищах Linux централізовані інструменти моніторингу, такі як ELK Stack, дозволяють збирати, агрегувати та аналізувати логи з багатьох систем в режимі реального часу. Що у свою чергу дозволяє виявляти аномалії в роботі системи та вживати відповідних заходів.

ELK Stack – це загальний стек програмного забезпечення, який використовується для централізованого збору, обробки, аналізу та візуалізації логів і даних інфраструктури ELK розшифровується як Elasticsearch, Logstash і Kibana та Beats ELK розшифровується як Elasticsearch, Logstash і Kibana і може також включати Beats Використовуючи ELK Stack, організації можуть ефективно відстежувати та аналізувати події в режимі реального часу, а також виконувати ретроспективний аналіз даних для виявлення проблем і вразливостей. Основними компонентами ELK Stack є:

Elasticsearch – це розподілена система управління даними для їхнього пошуку та аналізу. Вона використовує індексування та пошук для зберігання та вилучення великих обсягів структурованих та неструктурованих даних, таких як журнали подій. Elasticsearch дозволяє користувачам швидко досліджувати дані та витягувати з них інформацію.

Logstash – це система, яка збирає, обробляє і нормалізує журнали і дані з різних джерел, дозволяючи стандартизувати і обробляти дані перед

індексацією в Elasticsearch Logstash; підтримує різні журнали, бази даних і API Logstash; підтримує різні джерела вхідних і вихідних даних, включаючи журнали, бази даних і API.

Kibana Kibana – це інтерактивний веб-інтерфейс для візуалізації та аналізу даних, що зберігаються в Elasticsearch. Він дає можливість створювати діаграми, графіки, таблиці та інші візуалізації для аналізу журналів і подій; Kibana також надає можливість створювати запити і фільтри для подальшого вивчення даних.

Beats – це легкий агент, який можна встановити на сервер або клієнтську систему для збору та надсилання даних до Logstash та Elasticsearch. Існує Filebeat для збору логів файлів і Metricbeat для збору метричних даних.

ELK Stack – надає можливість централізовано збирати та аналізувати дані з різних джерел, виявляти аномалії та незвичну активність, створювати графіки та інсайти, а також легко здійснювати моніторинг та аналіз в режимі реального часу. Це потужний інструмент для моніторингу та аналізу подій в індустрії кібербезпеки та інших галузях, де моніторинг та аналіз великих обсягів даних є критично важливим.

Інструментарій Linux-систем

Інструменти для налагодження Linux-систем та пошуку вразливостей відіграють важливу роль у забезпеченні безпеки та виявленні потенційних загроз. Ось деякі з найпопулярніших інструментів цієї категорії [4, 5]:

GDB (GNU Debugger) є одним з найбільш широко використовуваних інструментів для налагодження програмного коду в Linux. Він дозволяє експертам з кібербезпеки аналізувати і налагоджувати програми, виявляти і виправляти вразливості безпеки. GDB використовуються для аналізу пам'яті, стеків викликів, регістрів та інших аспектів виконання програми. Можна дослідити критичні помилки та виявити вразливості.

Wireshark – це інструмент для аналізу мережевого трафіку. Він дозволяє експертам з кібербезпеки перехоплювати, аналізувати і контролювати пакети даних, що надсилаються через мережу. Wireshark можна використовувати для виявлення аномального мережевого трафіку, атак, перехоплення даних та інших мережевих загроз. Він надає інформацію про джерело і місце призначення пакетів, щоб можна було виявити аномалії.

Tcpdump – інструмент командного рядка для моніторингу мережевого трафіку. Він може аналізувати і записувати пакети даних, що надсилаються в мережі. За допомогою Tcpdump фахівці з кібербезпеки можуть відстежувати і аналізувати мережевий трафік в режимі реального часу. Його можна використовувати для виявлення атак, пошуку вразливостей і розслідування мережевих подій.

Nessus – комерційний інструмент для виявлення вразливостей в мережевих системах. Він сканує порти, аналізує вразливості системи і надає звіти. Nessus використовується для проактивного виявлення вразливостей системи, включаючи патчі та налаштування безпеки. Він допомагає експертам з кібербезпеки виявляти проблеми безпеки та рекомендувати заходи щодо їх усунення.

OpenVAS (Open Vulnerability Assessment System) – це програмне забезпечення з відкритим вихідним кодом для виявлення системних і мережевих вразливостей. Воно включає в себе базу даних вразливостей і сканер вразливостей. Використовуючи OpenVAS, експерти з кібербезпеки можуть проводити аудит систем для виявлення вразливостей і надавати звіти та рекомендації щодо їх усунення.

Nmap (Network Mapper) – це програмне забезпечення з відкритим вихідним кодом, яке сканує мережу та визначає активні хости і відкриті порти. Він також може виявляти служби, запущені на кожному порту, і надавати інформацію про операційну систему, яка використовується хостом. Використання Nmap допомагає експертам з кібербезпеки сканувати мережі для виявлення потенційних вразливостей і створювати картину мережі для виявлення активних пристроїв і сервісів.

Nikto – це інструмент, який сканує веб-сервери на наявність вразливостей і потенційних загроз, а також перевіряє веб-сайти на наявність відомих вразливостей і налаштувань безпеки. Nikto використовується для виявлення вразливостей у веб-додатках, веб-серверах та інших веб-ресурсах. Він надає звіти про знайдені проблеми і дозволяє адміністраторам виправити їх.

Burp Suite – це інтегроване середовище тестування безпеки веб-додатків, яке включає в себе різні інструменти, такі як Proxy, Scanner, Intruder і Repeater для виявлення вразливостей веб-додатків. Burp Suite використовується для тестування безпеки веб-додатків шляхом перехоплення і модифікації запитів і відповідей, виявлення вразливостей і автоматичного сканування веб-додатків.

Metasploit – це інструментарій для тестування на проникнення та експлуатації вразливостей. Він включає в себе широкий спектр модулів і експлойтів для тестування безпеки системи. Metasploit використовується для тестування вразливостей і системних уразливостей з метою виявлення потенційних проблем безпеки.

AIDE – це інструмент виявлення вторгнень, який може встановлювати контрольні суми для файлів та інших системних атрибутів, щоб виявити зміни в системі. AIDE можна використовувати для виявлення несанкціонованих змін у системних файлах та розслідування інцидентів.

OWASP ZAP – це безкоштовний інструмент тестування на проникнення до веб-додатків, який надає можливість блокувати та модифікувати HTTP-запити, виявляти вразливості та створювати детальні звіти. Використання OWASP ZAP допомагає експертам з кібербезпеки проводити тестування безпеки веб-додатків, виявляти вразливості та надавати рекомендації щодо їх усунення.

Hydra – це інструмент для атаки на паролі, який може виконувати атаки грубої сили (перебір, словникові атаки і т.д.) на різні протоколи і сервіси. Застосування Hydra використовується для перевірки стійкості паролів і виявлення слабких місць в системі безпеки шляхом виконання атак грубого перебору паролів.

Lynis – це інструмент для аудиту безпеки системи. Він сканує систему на наявність вразливостей безпеки та надає рекомендації щодо їх усунення. Використання Lynis допомагає експертам з кібербезпеки аналізувати системні налаштування, виявляти слабкі місця та забезпечувати безпеку.

Висновок

Отже виходячи з вищенаведеного ми можемо констатувати що Linux є важливою операційною системою для індустрії кібербезпеки та захисту інформаційних систем оскільки Linux пропонує численні переваги та є по суті та за змістом універсальним інструментом як для організацій так і для фахівців з кібербезпеки. Однією з головних переваг Linux є те, що він має відкритий вихідний код. Це означає, що спільнота користувачів може тестувати і перевіряти код, виявляти вразливості і застосовувати виправлення, а також робити систему більш стійкою до атак. Також Linux відома своєю стійкістю до різних типів атак, включаючи віруси, шкідливі програми та зловмисне програмне забезпечення. Відсутність антивірусного програмного забезпечення, яке часто вимагається в інших операційних системах, є свідченням внутрішньої безпеки Linux. Linux теж пропонує ряд можливостей для налаштування безпеки на різних рівнях, включаючи налаштування ядра, файлової системи та мережі. Це дозволяє фахівцям з кібербезпеки налаштовувати систему відповідно до своїх потреб. Linux можна інтегрувати з інструментами централізованого моніторингу та аналізу подій, такими як ELK Stack, щоб виявляти аномалії та атаки в режимі реального часу. Linux надає набір інструментів для налагодження та дослідження вразливостей, які допомагають фахівцям з кібербезпеки виявляти, аналізувати та виправляти вразливості. Linux має велику та активну спільноту користувачів та розробників, які надають підтримку та ресурси з питань безпеки.

Загалом, Linux використовується у сфері кібербезпеки як надійна, гнучка та потужна операційна система, яка допомагає фахівцям з кібербезпеки забезпечувати безпеку інфраструктури та даних. Відкритий вихідний код, гнучкість та багатий інструментарій Linux є важливими ресурсами для захисту від кібератак та вразливостей у цифровому просторі, а також Linux сприяє створенню безпечнішого онлайн-середовища, не лише виявляючи загрози та небезпеки, але й пом'якшуючи їхній вплив.

Література

1. Що краще: Linux чи Windows? Порівняння операційних систем. [Електронний ресурс]. – Доступний з https://acode.com.ua/linux-vs-windows/

2. Проект CentOS. [Електронний ресурс]. – Доступний з https://www.centos.org/

3. Red Hat – We make open source technologies for the enterprise. [Електронний ресурс]. – Доступний з https://www.redhat.com/en

4. Arch Linux. [Електронний ресурс]. – Доступний з https://archlinux.org/

5. The file systems of Linux. [Електронний ресурс]. – Доступний з https://www.ufsexplorer.com/uk/articles/ linux-file-systems/

УДК 004.056.55

ВИКОРИСТАННЯ ФРАКТАЛЬНОЇ ПОСЛІДОВНОСТІ ПРИ ЗАБЕЗПЕЧЕННІ ЗАХИСТУ ІНФОРМАЦІЇ

Васильєва Єва, Мацакова Анастасія
Національний університет цивільного захисту України, Харків

Анотація. Викладено принципову можливість використання фрактальних дробних розмірностей для забезпечення інформаційної безпеки при передачі інформації в інформаційних мережах. Запропоновано використовувати ключі у вигляді фрактальної послідовності із застосовуванням дробної фрактальної розмірності.

Ключова слова: інформаційна безпека, фрактальне шифрування, фрактальна розмірність.

Abstract. The fundamental possibility of using fractal small dimensions to ensure information security when transmitting information in information network has been outlined. A fractal sequence using a fractional fractal dimension as an encryption key parameter has been proposed.

Keywords: nformation security, fractal encryption, fractal dimension.

При сучасному цифровому розвитку в усіх галузях зростає залежність від використання технологій, смартфонів, комп'ютерів і Інтернету. Однак, зі збільшенням кількості інформації, яка обробляється й передається через мережі, зростає й ризик несанкціонованого доступу до неї з боку зловмисників. Щоб захистити дані, які передаються у мережі, від злочинців, повинно використовувати шифрування, щоб захистити цифрову інформацію. Важливою частиною алгоритмів шифрування є генератори випадкових чисел, які можуть ґрунтуватися на природних процесах.

Одним з альтернативних сучасних методів шифрування є метод фрактального шифрування, який використовує як кодуючу функцію фрактальну послідовність [1]. Найбільш застосовні і вивчаються безлічі Мандельброта і Жюлі, Басейни Ньютона [2].

Фрактальну послідовність одержують за допомогою ітераційної функції, яка у свою чергу є однобічною функцією, у таких функцій визначення аргументів за значенням самої функцій не може бути зроблене більш ефективно, ніж перебором по безлічі значень початкових параметрів [3]. Для опису ітераційної функції, досить указати набір дійсних чисел, які задають початкові умови ітераційного процесу побудови фрактальної послідовності. Це дає досить простий метод шифрування, він є варіантом гамірування – процесу "накладення" гама-послідовності на відкриті дані [4], де в якості гама-послідовності (послідовності псевдовипадкових елементів) використовується фрактальна послідовність, що генерується за допомогою ітераційної функції за початковими параметрами [5]. При цьому обчислення аргументу за значенням функції є завданням, за складністю, близьким до повного перебору.

За допомогою фракталів може бути підвищена стійкість алгоритмів шифрування за рахунок генерації необмежено довгих ключів. Також ще одна сфера застосування - візуальна криптографія. Фрактальна послідовність може формувати матрицю, яка діє на пікселі за деяким правилом, здійснюючи тим самим шифрування зображення.

Процес шифрування даних можна уявити з допомогою наступної формули:

$$E(M) = C, \quad (1)$$

а процес дешифрування

$$D(E(M)) = D(C) = M, \quad (2)$$

де M –відкритий текст (він має бути представлений у вигляді потоку бітів, причому спочатку це може бути текстовий файл, зображення, звук і т.д.), C – шифротекст, E – функція шифрування, D – функція дешифрування. Приклад фрактального шифрування схематично наведено на рисунку.

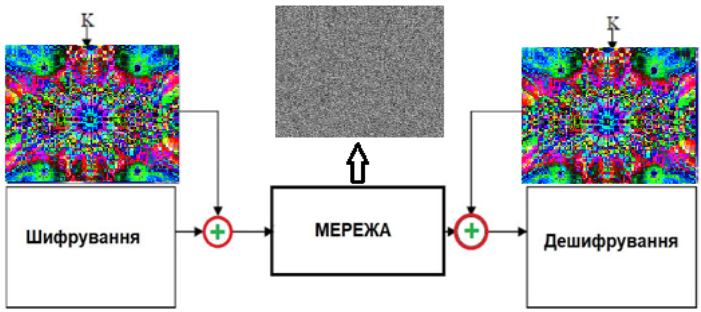


Рисунок 1 – Процес фрактального шифрування (К-ключ)

Алгоритм шифрування текстів за допомогою алгебраїчних фракталів складається з наступних кроків:

– перший, – символ тексту займає *1* байт;

– другий, – ключ формується за умови (кількість символів у фрактальному зображенні (див. рисунок) повинна бути більше або дорівнює кількості символів у тексті). На цьому етапі пропонується додатково визначити фрактальну розмірність потоку символів, для подальшого ускладнення перетворення шифру;

– третій, використати процес, який наведено у формулі

$$a_i = \begin{cases} r_i AND\ g_i, i = 1,3,5,7 \\ r_i\ AND\ b_i, i = 0,2,4,6 \end{cases} \quad (3)$$

де a_i – елемент тексту(символ), що кодується; r_i, g_i й b_i – біти фрактального зображення за кольорами. Або виконати операцію *XOR* між бітами r_i, g_i й b_i, i =0,...,7.

Завдяки перетворенням, виходить необхідна послідовність, що шифрує, між якою й потоком бітів, що шифрується тексту застосовується операція XOR. Потім біти перетворюються у символи. Тому що алгоритм є симетричними, дешифрация даних проводиться у зворотному порядку з тим же ключем з додатковою операцією з використанням значення фрактальної розмірності.

Таким чином, використання фрактальних послідовностей як ключа для шифрування достатньо просте й ефективне. Для їх побудови необхідна невелика кількість параметрів, при цьому на виході формуються об’єкти зі складними хаотичними межами. Також, ефективно та зручно використовувати фрактальні послідовності для шифрування текстової інформації, представленої як у графічному вигляді, так і в символьному.

Література

1. Mandelbrot, B. The Fractal Geometry of Nature. USA: Echo Point Books & Media, LLC. 2021. 500 p. DOI: https://doi.org/10.1119/1.13295.

2. Anand, Rubesh & Bajpai, Gaurav & Bhaskar, Vidhyacharan. (2009). Real-Time Symmetric Cryptography using Quaternion Julia Set.

3. Soumitro Banerjee. Fractal Image Compression. Available at: https://youtu.be/Lte3xpmH2_g (accessed 23.03.2023).

4. Xian Y., Wang X. Fractal sorting matrix and its application on chaotic image encryption //Information Sciences. – 2021. – Т. 547. – С. 1154-1169.

5. Chen G., Ueta T. Yet another chaotic attractor //International Journal of Bifurcation and chaos. – 1999. – Т. 9. – №. 07. – С. 1465–1466.

УДК 355.58

ПРОБЛЕМИ ГЕНДЕРНОЇ РІВНОСТІ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Верхолюк Юлія
Львівський державний університет безпеки життєдіяльності, м. Львів

Кількість інтернет-користувачів за останні 10 років збільшилася більш ніж удвічі — з 2,18 млрд. У свою чергу стрімкий розвиток інформаційно-комунікаційних технологій відкриває нові шляхи для насильства проти жінок і дівчат. Тому і зростає необхідність у розгляді питань, щодо проблем гендерної рівності в інтернет-ресурсах.
Ключові слова: гендер, безпека, рівність, Інтернет.

The number of Internet users has more than doubled over the past 10 years, from 2.18 billion. In turn, the rapid development of information and communication technologies opens new avenues for violence against women and girls. That is why there is a growing need to consider issues of gender equality in Internet resources.
Key words: gender, safety, equality, Internet.

Інтернет є невід'ємною частиною нашого суспільства і все частіше сприймається як одне з основних прав людини. Поява цифрових технологій надала більше різних можливостей для використання своїх здібностей, покращення якості життя, саморозвитку та внеску у добробут суспільства. Проте всім відомо, що між можливостями чоловіків і жінок є певні відмінності, що змушують зачепити питання рівності.

Гендерна рівність означає, що всі людські істоти мають свободу для розвитку своїх особистих здібностей та свободу вибору без обмежень, пов’язаних із жорстко закріпленими гендерними ролями. Тобто різна поведінка, прагнення та потреби жінок і чоловіків враховуються, оцінюються й підтримуються рівним чином [1].

З 2019 року показник гендерного паритету покращився, однак абсолютна різниця між числом чоловіків та жінок, які користуються Інтернетом, фактично збільшилася на 20 мільйонів. У 2022 році Інтернетом у всьому світі користувалися 63 відсотки жінок та 69 відсотків чоловіків . Жінки на 12 відсотків рідше, ніж чоловіки, володіють мобільним інтернетом, і цей показник практично не змінився з 2019 року.[2] Що стосується жінок в ситемі ІТ-частка жінок в українському ІТ не змінилася за рік — 23% , в українській ІТ-сфері працює близько 240 тисяч чоловіків і понад 71 тисяча жінок [3].

Намагаючись подолати ці бар’єри гендеру, жінки часто зазнають дискримінації та навіть насильства. Як з’ясувалося під час опитування, 63% ІТ-спеціалісток в Україні не знають, скільки заробляють колеги на тій самій посаді та з тим самим рівнем досвіду. Це свідчить про проблеми з прозорістю в більшості компаній-роботодавців. Наразі жінки в Європейському Союзі заробляють в середньому на 13% менше, ніж чоловіки, а українки майже на 18,4% [4].

Звичайно, і чоловіки можуть стикатися з проявами порушення інформаційної безпеки, однак жінки більшою мірою зазнають даного негативного впливу. Жорстке поводження з жінками в онлайн-середовищі змушує багатьох із них відмовитися від користування інтернетом, зокрема від висловлення своєї думки на онлайн-платформах. Це особливо проблематично для захисниць прав жінок і дівчат, журналісток або тих, хто займається політикою, а також для

впливових лідерок думок у соціальних мережах та інших осіб, які працюють у соціальних мережах та/або є публічними особами [5]. У такий спосіб насильство над жінками й дівчатами в цифровій сфері приглушує їхні голоси та зменшує можливість участі в публічних дебатах. Опитування (2022-2023) журналісток зі 125 країн показав, що в ході своєї роботи 73 відсотки респонденток зазнавали насильства в Інтернеті, при цьому 30 відсотків повідомили, що в результаті цього їм довелося піддати себе само цензурі. Це в свою чергу, обмежує їх участь у суспільному житті та підриває демократію та права людини [2].

Звісно ж, ці події привернули до себе увагу, почали з'являтися нові закони та проекти. 20 червня 2022 року Україна ратифікувала Конвенцію Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами (Стамбульську конвенцію).

8 березня 2022 року Європейська комісія схвалила пропозицію до директиви щодо боротьби з насильством проти жінок і домашнім насильством. Пропозиція має на меті забезпечити кримінальну відповідальність за найсерйозніші форми насильства щодо жінок у всьому ЄС. Туди також входять і ґендерно зумовлене кібернасильство, включно з кіберпереслідуванням та обміном інтимними зображеннями без наданої на це згоди [6].

Наразі, політика в сфері інформаційної безпеки не стоїть на місці, однак і далека до досконалості. А нерівності між статтями у цій сфері та й загалом у всіх сферах життєдіяльності, зможе знайти рівновагу лише за умови поступової трансформації світоглядних настанов усіх громадян, залучення чоловіків, на рівні із жінками, до участі в просуванні ідей ґендерної рівності, реалізації заходів із протидії та попередження насильства щодо жінок та чаловіків. Адже гендер – це глобальна проблема, що стосується кожного.

Література

1. Ґендерна рівність[Електронний ресурс]. – Режим доступу: https://nssu.gov.ua/genderna-rivnist

2. United Nations, Commission on the Status of Women Sixty-seventh session [Електронний ресурс]. – Режим доступу: https://nssu.gov.ua/genderna-rivnist – с.3, 16

3. Стало відомо, скільки жінок працює в українському IT і яка в них спеціалізація [Електронний ресурс]. – Режим доступу: https://www.unian.ua/economics/other/stalo-vidomo-skilki-zhinok-pracyuye-v-ukrajinskomu-it-i-yaka-v-nih-specializaciya-12291072.html

4. Жінки в IT в Україні та низці країн ЄС заробляють менше чоловіків [Електронний ресурс]. – Режим доступу: https://ain.ua/2023/03/19/skilky-zaroblyayut-zhinky-v-it-v-ukrayini-ta-nyzczi-krayin-yes-spojler-menshe-nizh-choloviky/

5. Загальна рекомендація ГРЕВІО № 1 щодо цифрового виміру насильства стосовно жінок [Електронний ресурс]. – Режим доступу: https://rm.coe.int/grevio-2021-20-first-general-recommendation-ukr/1680a4ad92

6. Насильство проти жінок: Європейський Союз відкриває спільну телефонну лінію довіри ЄС та закликає покласти край насильству щодо жінок в усьому світі[Електронний ресурс]. – Режим доступу: https://www.eeas.europa.eu/delegations/ukraine/насильство-проти-жінок-європейський-союз-відкриває-спільну-телефонну-лінію-довіри-єс-та-закликає_uk?s=232

УДК 004.07.022

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Гелешко Ірина, Ящук Валентина, Навитка Марія
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи використання системи блокчейн у системах електронного голосування. визначено сучасні підходи до впровадження системи блокчейн у системах електронного голосування у різні галузі народного господарства. наведено методичні підходи до формування концепції використання системи електронного голосування. проаналізовано переваги та недоліки використання системи електронного голосування у різних галузях господарства.

Ключові слова: системи електронного голосування, забезпечення безпеки, технологія блокчейн.

The theoretical, scientific-methodical and organizational-functional bases of using the blockchain system in electronic voting systems are considered. modern approaches to the implementation of the blockchain system in electronic voting systems in various sectors of the national economy are defined. methodical approaches to the formation of the concept of using the electronic voting system are given. the advantages and disadvantages of using the electronic voting system in various branches of the economy are analyzed.

Keywords: electronic voting systems, security, blockchain technology.

Сьогодні, в еру інформаційного прогресу, постійного оновлення програмного забезпечення та оцифровування інформації все більшою популярністю користуються системи електронного голосування. Електронне голосування є надзвичайно актуальним для України, оскільки відповідає всім сучасним вимогам демократичного суспільства. Воно дозволяє розширити доступ громадян до виборів, підвищити їхню явку, а також зробити процес голосування більш зручним та безпечним. Електронне голосування – це спосіб голосування, при якому всі етапи процесу – від волевиявлення до підрахунку голосів – здійснюються за допомогою електронних засобів.

Кожна технологія електронного голосування має свої переваги та недоліки. Наприклад, електронні машини для голосування можуть спростити процес голосування та прискорити підрахунок голосів, але вони також можуть бути більш вразливими до кібератак. Щоб впровадити електронне голосування на національному рівні, необхідно враховувати як переваги, так і недоліки різних технологій. Також важливо розробити надійні системи безпеки, які захистять процес голосування від кібератак та інших

видів зловживань. У кінцевому підсумку, електронне голосування має бути прийнятним для всіх учасників виборчого процесу, як для виборців, так і для органів влади. Тільки за таких умов можна гарантувати, що результати виборів будуть достовірними та визнаними всіма сторонами.

Останніми роками в світі з'явилося багато нових електронних технологій, які підвищують якість нашого життя, надають нові сервіси та послуги, зменшують ризики негативних подій та пом'якшують можливі наслідки. Одна із таких технологій – блокчейн. Децентралізація в блокчейні [1, 2] реалізується через складні та пов'язані між собою криптографічні механізми, які гарантують, що події, які вже відбулися та задокументовані, не можуть бути змінені чи скомпрометовані. В таких системах неможливо заднім числом ввести додаткове мито чи змінити звітність, неможливо скасувати борг або обвалити курс національної валюти. Блокчейн-системи – це захищені сховища, в яких забезпечується історично стійке зберігання записів (реєстрів), і ці реєстри можуть містити будь-яку важливу інформацію. Вся ця інформація не може бути змінена, ця інформація історично захищена, незмінна, неспростовна і це надає можливість для якісно нового стану – незалежності та свободи. Історично стійке збереження кожного результату волевиявлення особистості забезпечує свободу та незалежність голосування спільноти.

За ступенем автоматизації системи електронного голосування можна поділити на такі, що: застосовують для підрахунку голосів електронні пристрої, що зчитують відмітки з паперових бюлетенів; застосовують машини для голосування з електронними дисплеями та кнопками (або сенсорними дисплеями) замість паперових бюлетенів; результати голосування зберігаються у пам'яті машини для голосування; реалізують дистанційне (віддалене) голосування через мережу Інтернет із використанням криптографічних протоколів. За принципом побудови віддалені системи електронного голосування поділяються на централізовані та децентралізовані.

Представники громадянського суспільства, міжнародні експерти та інші зацікавлені сторони висловили занепокоєння щодо можливого пілотного проекту Інтернет-голосування під час виборів до органів місцевого самоврядування [3]. Серед причин, що створюють перепони для пілотування Інтернет-голосування у найближчій перспективі:

1) відсутність необхідної технологічної інфраструктури для проведення ефективного пілотного Інтернет-голосування;

2) високий ризик технічних збоїв та кібератак, особливо в контексті триваючого військового конфлікту, недавніх витоків особистої інформації громадян з державних реєстрів;

3) відсутність системи електронного урядування з високим ступенем довіри громадськості, а також відповідної інфраструктури по всій країні;

4) брак надійної системи цифрової ідентифікації;

5) значний рівень недовіри до Інтернет-голосування з боку виборців та політиків, що може стати на заваді визнання результатів Інтернет-голосування;

6) невдале пілотування матиме негативні наслідки для всіх технологічних ініціатив в галузі електронної демократії в Україні, до яких громадяни можуть втратити довіру.

Побудова системи електронного голосування на основі блокчейну [2] дозволить забезпечити виконання таких властивостей як: прозорість: достовірність транзакції, що містить голос виборця, може бути перевірена учасниками протоколу голосування у будь-який момент; цілісність: транзакція, що містить голос виборця, не може бути модифікована або вилучена з блокчейну після того, як блок, в якому міститься ця транзакція, було прийнято у результаті консенсусу; анонімність голосування, що не дозволяє зв'язати транзакцію, що містить голос виборця, з його особою (ідентифікаційними даними); автоматичний підрахунок голосів та публікація результатів голосування.

Впровадження технології блокчейн підвищує довіру до інформаційних ресурсів, надійність збереження інформації та якість наданих послуг. В Україні технологія блокчейн вже знайшла застосування при розробці електронних реєстрів. На сьогодні голосування на блокчейні не набуло широкого впровадження державними інституціями, проте є приклади таких протоколів та їх застосування на приватному рівні. З огляду на сказане та в контексті реалізації плану "Держава у смартфоні", на нашу думку, розробку системи електронного голосування, що базуватиметься на використанні технології блокчейн, найперспективнішим варіантом розбудови національної системи електронного голосування.

Література

1. Горбенко І.Д., Кузнецов О.О., Потій О.В., Горбенко Ю.І., Полуяненко М.О. Технологія блокчейн: огляд, сучасні проблеми та перспективи впровадження в Україні // ІІ міжнар. наук.-практ. конф. "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS), 11-12 квітня 2019 р., м. Київ, 2019. С. 217-220.

2. Isirova K., Potii O. Decentralized public key infrastructure development princi-ples // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Kiev, 2018. P. 305-310.

3. Спільна заява щодо пілотування Інтернет-голосування під час місцевих виборів у жовтні 2020 року [Електронний ресурс]. – Режим доступу: https://www.oporaua.org/statement/vybory/20122- spilna-zaiava-shchodo-pilotuvannia-internet-golosuvannia-pid-chas-mistsevikh-viboriv-u-zhovtni-2020- roku Національний інститут стратегічних досліджень.

УДК 004.07.022

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІТ СИСТЕМАХ ТА МЕРЕЖАХ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Гетьман Арсеній, Ткачук Ростислав
Львівський державний університет безпеки життєдіяльності, Львів

Анотація: З урахуванням стрімкої динаміки розвитку технологій та широкого застосування інформаційних технологій у всіх сферах суспільства, виникає необхідність ефективного захисту персональних даних, які зберігаються та обробляються в інформаційних технологіях (ІТ) та мережах об'єкту інформаційної діяльності. Зростання кількості кіберзагроз, крадіжок особистої інформації та несанкціонованого доступу до конфіденційної інформації ставить під загрозу приватність і безпеку користувачів.

Основні ключові слова: Захист персональних даних, інформаційна безпека, ІТ системи, мережі, дослідження уразливостей, кібербезпека, конфіденційність, інформаційна діяльність, рекомендації з безпеки, ідентифікація та аутентифікація.

Abstract: given the rapid dynamics of technology development and the widespread use of information technology in all spheres of society, there is a need for effective protection of personal data stored and processed in information technology (IT) and networks of the information activity object. The growing number of cyber threats, identity theft and unauthorized access to confidential information jeopardizes the privacy and security of users.

Key words: Personal data protection, information security, IT systems, networks, vulnerability research, cybersecurity, confidentiality, information activity, security recommendations, identification and authentication.

Аналіз сучасного стану кіберзагроз та існуючих викликів у сфері захисту персональних даних передбачає оцінку поточного стану безпеки інформаційних систем та мереж, які обробляють та зберігають персональні дані. Це дослідження зазвичай включає такі ключові елементи [1–3, 5]:

1. Аналіз загроз, на цьому етапі проводиться моніторинг актуальних загроз кібербезпеці, які можуть впливати на конфіденційність персональних даних. Цей етап включає вивчення відомих типів атак, розповсюджених методів інтелектуального вторгнення, а також ідентифікацію потенційних небезпек.

2. Оцінка вразливостей, на цьому етапі виявляють найкритичніші (найслабші) місця у системах та мережах, які можуть бути використані для несанкціонованого доступу до персональних даних. Проведення вивчення на даному етапі може включати і аналіз експлуатації програмних та апаратних вразливостей.

3. Вивчення сучасних викликів, на цьому етапі проводиться огляд сучасних тенденцій і викликів у сфері кіберзахисту, таких як розширення кількості та складності атак, зростання значущості соціальної інженерії, та зміни законодавства щодо захисту особистих даних.

4. Аналіз стану захисту – перевіряється ефективність наявних заходів безпеки в організації, а саме: системи виявлення та запобігання вторгнень, системи моніторингу та аудиту безпеки.

5. Оцінка дотримання стандартів, політик, рекомендацій – реалізується перевірка на відповідність наявної практики захисту персональних даних в організації до вимог відповідних законодавчих актів та стандартів.

Загалом основна ціль у проведенні такого аналізу полягає у визначенні слабких місць у системах захисту та подальшій розробці рекомендацій спрямованих на підвищення безпеки персональних даних у сучасному цифровому середовищі.

Розробка конкретних рекомендацій та стратегій для підвищення ефективності захисту персональних даних в IT системах та мережах об'єкта інформаційної діяльності, як правило, включає в себе декілька ключових етапів та заходів [1, 4, 6]:

1. Аудит безпеки:
– оцінка існуючих заходів – проведення аудиту безпеки для визначення ефективності поточних заходів захисту персональних даних;
– ідентифікація слабких місць – виявлення вразливостей та слабких місць у наявних системах та мережах.
2. Визначення стратегії безпеки:
– розробка стратегії захисту – визначення цілей та завдань стратегії безпеки для забезпечення конфіденційності, цілісності та доступності персональних даних;
– проектування мережевої архітектури – розробка оптимальної мережевої структури для максимального захисту персональних даних.
3. Впровадження технічних заходів:
– вдосконалення систем безпеки – проведення апгрейду або встановлення нових систем виявлення та запобігання вторгнень, антивірусних та антишпигунських рішень;
– шифрування даних – застосування механізмів шифрування для забезпечення конфіденційності даних під час їхньої передачі та зберігання.
4. Розробка політик та процедур безпеки:
– створення правил доступу – встановлення строгих правил доступу до персональних даних для обмеження доступу лише до необхідної інформації;

– проведення тренінгів (навчання) персоналу – ознайомлення персоналу з правилами та процедурами захисту даних для мінімізації внутрішніх загроз.

5. Забезпечення відповідності:

– впровадження стандартів безпеки – дотримання встановлених стандартів та вимог законодавства з охорони персональних даних;

– розробка механізмів моніторингу та звітності – встановлення систем моніторингу для відстеження та звітності щодо подій, пов'язаних з безпекою.

6. Постійне вдосконалення:

– аналіз інцидентів – проведення ретельного аналізу інцидентів безпеки для вдосконалення стратегій та процедур;

– проведення регулярних аудитів та тестів безпеки – проведення регулярних аудитів та тестів для забезпечення постійного покращення систем захисту.

Перевірка ефективності рекомендацій на практиці та їх адаптація відповідно до специфіки об’єкту інформаційної діяльності – це ключовий етап у процесі впровадження заходів спрямованих на захист персональних даних [5–7]. Цей процес включає в себе декілька важливих аспектів:

1. Створення тестового середовища – розробка імітаційного середовища, яке відображає реальні умови об’єкту інформаційної діяльності; створення сценаріїв, які відображають різноманітні кіберзагрози та ситуації, що можуть виникнути підчас роботи.

2. Впровадження рекомендацій – застосування розроблених рекомендацій та стратегій до тестового середовища; визначення, як рекомендації взаємодіють з існуючими системами та процедурами.

3. Моніторинг та аналіз – систематичний моніторинг реакції на рекомендації у реальному часі; збір та аналіз даних щодо застосування рекомендацій у різних сценаріях.

4. Оцінка ефективності – визначення ефективності рекомендацій щодо попередження інцидентів безпеки та мінімізації можливих наслідків; аналіз зменшення ризиків та ідентифікація можливих вдосконалень.

5. Адаптація до специфіки – врахування унікальних особливостей об’єкту інформаційної діяльності; виправлення недоліків та модифікація рекомендацій, якщо це необхідно для оптимального використання у конкретному середовищі.

6. Навчання персоналу – організація навчальних заходів для персоналу щодо нових стратегій та процедур; виокремлення деталей адаптації та визначення важливості їхнього використання в контексті організації робочих процесів об’єкту інформаційної діяльності.

Впровадження та дотримання вище наведених заходів є хорошою практикою для забезпечення високого рівня захисту персональних даних в

ІТ системах та мережах об'єктів інформаційної діяльності. Також слід зауважити що реалізація таких заходів не може вважатися достатньою за умови разового впровадження, тому такі заходи потребують постійного вдосконалення та періодичного проведення навчання з персоналом. І тільки за таких умов та підходів можна забезпечити ефективне управління кібербезпекою в сучасному інформаційному середовищі.

Література

1. Web Server and its Types of Attacks. – https://www.greycampus.com/opencampus/ethicalhacking/ web-server-and-its-types-of-attacks.

2. Brewer J. Web Server Vulnerabilities and a Defense in Depth Strategy Using the Squid Proxy / Jim Brewer // GSEC Practical version 1.4b. – 2004.

3. Web Vulnerability Scanner v10 Product Manual – http://www.acunetix.com/resources/wvsmanual.pdf

4. Acunetix Web Vulnerability Scanner http://www.securitylab.ru/software/266415.php

5. Дослідження вразливостей Web-сайтів та методів їх усунення. – http://phone.kpi.ua/wpcontent/uploads/ 2014/06/4.pdf

6. Потенційні вразливості брандмауера. Філіпчук Б., Ткачук Р.Л., Репетило Т.Б. Зб. тез доп. IV Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології". (м. Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 111-114.

7. Організація оперативного управління кібербезпекою компанії. Мних М., Ткачук Р.Л., Федина Б.І. Зб. тез доп. IV Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології". (м. Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 30-32.

УДК 004.07.022

МЕРЕЖЕВИЙ АУДИТ ЯК ІНСТРУМЕНТ ВИЗНАЧЕННЯ ВРАЗЛИВОСТЕЙ СЕРВЕРІВ ТА РОБОЧИХ СТАНЦІЙ

Гетьман Арсеній, Фединець Наталія
Львівський державний університет безпеки життєдіяльності, Львів

Анотація: В одному з аспектів забезпечення безпеки інформації важливе місце займає мережний аудит. Мережний аудит - це процес оцінки мережевого середовища для ідентифікації потенційних вразливостей та слабких місць, які можуть бути використані для атак та порушень безпеки. В даній презентації ми глибше розглянемо важливість мережного аудиту, різні методи та інструменти, які використовуються для визначення вразливостей серверів та робочих станцій, та приклади його успішного використання в реальних сценаріях.

Ключові слова: мережний аудит, інструменти мережного аудиту, захист від зовнішніх загроз, мережеві порти, аналіз вразливостей, аудит конфігурацій, усунення вразливостей.

Abstract: In one of the aspects of ensuring information security, network audit occupies an important place. Network auditing is the process of evaluating the network environment to identify potential vulnerabilities and weak points that can be exploited for attacks and security breaches. In this presentation, we will take a deeper look at the importance of network auditing, the various methods and tools used to identify server and workstation vulnerabilities, and examples of its successful use in real-world scenarios.

Keywords: network audit, network audit tools, protection against external threats, network ports, vulnerability analysis, configuration audit, vulnerability elimination.

Сервери та робочі станції є основними мішенями для зловмисників, що намагаються незаконно отримати доступ до систем та даних. Мережний аудит дозволяє виявити потенційні вразливості, що можуть бути використані для атак, і приймати заходи для їхнього усунення.

Іноді загрози можуть виникати від власних співробітників або інших авторизованих користувачів. Мережний аудит допомагає виявити недоречності в налаштуваннях та діях користувачів, що може запобігти внутрішнім загрозам.

У багатьох галузях, таких як фінанси, охорона здоров'я та галузі, пов'язані з обробкою особистих даних, існують суворі вимоги щодо забезпечення безпеки та конфіденційності даних. Мережний аудит допомагає підтримувати відповідність з регуляторними стандартами.

Методи та інструменти мережного аудиту [1–3]:

1. Сканування портів (Port Scanning): Сканування портів дозволяє визначити, які мережеві порти відкриті та доступні для з'єднань. Наприклад, програми, такі як Nmap, дозволяють ідентифікувати служби, які працюють на окремих портах.

2. Аналіз вразливостей (Vulnerability Assessment): Використання спеціалізованих інструментів для виявлення вразливостей, таких як Nessus або OpenVAS. Ці інструменти проводять тестування на наявність вразливостей та надають звіти про їхню важливість та шляхи виправлення.

3. Аудит конфігурації (Configuration Auditing): Перевірка налаштувань серверів та робочих станцій на предмет відповідності безпечним налаштуванням та рекомендаціям з безпеки. Наприклад, інструменти, які перевіряють групові політики в системах Windows або файли конфігурації Linux.

Приклади використання мережного аудиту:

1. Захист від DDoS-атак: Мережний аудит може допомогти виявити збої в інфраструктурі під час атак типу DDoS та надати можливість приймати заходи для зменшення їх впливу.

2. Виявлення несанкціонованого доступу: Мережний аудит допомагає виявляти незвичайні дії користувачів або спроби несанкціонованого доступу до систем.

3. Усунення слабких місць в архітектурі мережі: Мережний аудит може допомогти виявити проблеми в мережевій архітектурі, такі як надмірне використання старих протоколів, неактуальні апаратні рішення та інші слабкі місця.

Мережний аудит є невід'ємною складовою стратегії забезпечення безпеки мережевого середовища та визначення вразливостей серверів та робочих станцій. Використання методів та інструментів мережного аудиту допомагає підвищити рівень безпеки, виявити потенційні загрози та приймати заходи для їхнього усунення. У світі, де інформаційна безпека стає ключовою проблемою, мережний аудит визначення вразливостей серверів та робочих станцій є важливим інструментом для забезпечення цілісності, конфіденційності та доступності інформації.

Література

1. Гавриленко А.С. Аудит інформаційної безпеки в комп'ютерних мережах на базі Mikrotik. 2019. UR: openarchive.nure.ua.

2. Колісниченко М.А. Аудит інформаційної та кібербезпеки в вищих навчальних закладах України». 2018. URL: ir.nmu.org.ua.

3. Чунарьова А.В. Сучасні методи аудиту та моніторингу в задачах захисту інформації. Проблеми інформатизації та управління. URL: jrnl.nau.edu.ua.

УДК 351.751+004.056.5

ЄВРОПЕЙСЬКИЙ КОНЦЕПТ ПРОТИДІЇ ДЕЗІНФОРМАЦІЙНИМ ПРОЯВАМ У ДЕРЖАВНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Глобенко Сергій
Інститут державного управління та наукових досліджень з цивільного захисту (м.Київ)

Анотація. Сфера інформаційної діяльності та захисту інформаційного простору стає дедалі важливішою в умовах загроз та кризових ситуацій, що є ключовим для національної стійкості. Держави докладають зусиль для розробки інструментів та заходів задля захисту власного інформаційного простору. Розглянуті ініціативи акцентують увагу на важливості прозорості, різноманітності, достовірності і інклюзивних рішень для забезпечення стійкості інформаційного простору.

Ключові слова: інформаційний простір держави, інформаційна безпека, захист інформаційного простору, державна політика в інформаційній сфері.

Abstract. The sphere of information activity and protection of the information space are becoming increasingly important in the face of threats and crises, which are crucial for national resilience. States are making efforts to develop tools and measures to safeguard their information space. The discussed initiatives emphasize the importance of transparency, diversity, credibility, and inclusive solutions to ensure the resilience of the information space.

Key words: information space of the state, information security, protection of information space, state policy in the information sphere.

Сьогодні сфера інформаційної діяльності й захисту інформаційного простору держави загалом, а також в умовах загрози чи виникнення надзвичайних і кризових явищ зокрема набуває особливої ваги, адже інформаційні чинники в публічному управлінні на шляху до забезпечення сталості розвитку держав світу характеризуються значним як консолідуючим, так і дестабілізуючим потенціалом. Недооцінювання чи нехтування ними може призвести до непоправних втрат – ресурсних, іміджевих, репутаційних тощо.

Розуміючи важливість і складність порушених питань, держави світу намагаються віднаходити дієві інструменти й вживати ефективних заходів задля забезпечення захисту власного інформаційного простору.

Зокрема, Європейська комісія [1, с. 7–8] вважає такими наступне.

По-перше, має бути забезпечена максимальна прозорість як щодо походження інформації, так і щодо того, яким чином вона генерується, ким спонсорується, поширюється та націлюється, аби надати можливість громадянам краще розуміти контент і виявляти ймовірні спроби маніпулювання чи дезінформування.

По-друге, сприяння різноманітності інформації, аби громадяни могли приймати обґрунтовані рішення на основі критичного аналізу (зокрема шляхом просування високоякісної журналістики, підвищення рівня власної медіаграмотності та зменшення дисбалансу у відносинах між творцями та розповсюджувачами інформації).

По-третє, підвищення рівня достовірності інформації шляхом надання доказів її надійності (зокрема через довірених інформаторів) і кращого відстеження та автентифікації впливових постачальників інформації.

По-четверте, пошук інклюзивних, комплексних рішень. Ефективні довгострокові рішення вимагають підвищення обізнаності, рівня медіаграмотності, широкого залучення зацікавлених сторін і співпраці між представниками державного й недержавного секторів.

Окрім вже згаданих підходів, окремі країни здійснюють заходи регіонального рівня, спрямовані на забезпечення ефективного функціонування власного державного інформаційного простору. Так, зокрема, відповідно до Постанови Ради міністрів про заснування посади Урядового уповноваженого з питань безпеки інформаційного простору Республіки Польща [2] до завдань відповідної посадової особи віднесено:

1. Координацію діяльності органів державного управління, до компетенції яких входить виявлення, моніторинг та нейтралізація інформаційних загроз інтересам держави, у сфері розпізнавання та нейтралізації загроз безпеці інформаційного простору держави та реагування на них. До таких загроз, зокрема, належать:

– виявлення та аналіз інформаційної діяльності, основним фокусом якої є безпека, інтереси та імідж Республіки Польща;

– ідентифікація суб'єктів, особливо іноземних, які організовують та провадять інформаційну діяльність всупереч інтересам Республіки Польща;

– відстеження проявів інформаційно-психологічних операцій, які проводяться в інформаційному просторі проти держави;

– проведення заходів, спрямованих на нейтралізацію виявлених загроз безпеці інформаційного простору Республіки Польща;

– реалізація заходів щодо підвищення стійкості інформаційного простору держави шляхом:

а) публікації досліджень з питань забезпечення безпеки інформаційного простору держави;

б) провадження інформаційної діяльності, спрямованої на зміцнення безпеки, інтересів та іміджу держави;

в) координації інформаційно-комунікативної діяльності установ, відповідальних за формування інформаційної політики Республіки Польща.

2. Розроблення рекомендацій для Ради міністрів задля пошуку системних рішень, метою яких є підвищення здатності Республіки Польща протистояти інформаційним загрозам.

Аналіз повноважень Урядового уповноваженого з питань безпеки інформаційного простору Республіки Польща свідчить, що подібна посадова особа за своїми функціональними обов'язками охоплює досить широкий контекст щодо захисту інформаційного простору держави як загалом, так і в умовах загрози чи виникнення надзвичайних і кризових явищ зокрема. Це дає підстави зробити припущення, що заснування подібних посад в інших державах і поширення позитивного досвіду окремих країн у рамках загального підходу Європейського співтовариства може призвести до суттєвих позитивних зрушень у напрямку забезпечення національної стійкості в інформаційній сфері держави.

Література

1. Bekämpfung von Desinformation im Internet: ein europäisches Konzept: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. COM(2018) 236 final. 26.04.2018. Brüssel, 2018. 21 S.

2. Rozporządzenie Rady Ministrów w sprawie ustanowienia Pełnomocnika Rządu do spraw Bezpieczeństwa Przestrzeni Informacyjnej Rzeczypospolitej Polskiej z dnia 11 sierpnia 2022 r. *Dziennik Ustaw Rzeczypospolitej Polskiej*. 17 sierp. 2022 r. Poz. 1714. S. 1–2.

УДК 316.346.2

ЗАХИСТ ПРИВАТНОСТІ ТА ІНФОРМАЦІЙНА БЕЗПЕКА В КОНТЕКСТІ ГЕНДЕРНОЇ ІДЕНТИЧНОСТІ

Гончаренко Марія
Львівський державний університет безпеки життєдіяльності, м. Львів

Анотація. Захист приватності та інформаційна безпека стали важливими аспектами в діалозі про гендерну ідентичність. Ідентифікація і вираз гендеру можуть бути надзвичайно особистими і чутливими аспектами для кожної людини. У цьому контексті забезпечення приватності та інформаційної безпеки для осіб, які виражають нетрадиційну гендерну ідентичність, стає додатковою важливістю.

Дослідження включає в себе аналіз сучасних методів та практик забезпечення інформаційної безпеки для гендерно різних осіб, а також розглядає законодавчі та етичні аспекти, пов'язані з цією темою. Також розглядаються способи захисту приватності і особистих даних у цьому контексті та важливість підтримки гендерно різних осіб у вирішенні цих питань.

Ключові слова: інформаційна безпека, гендер, гендерна ідентичність.

Abstracts .Privacy protection and information security have become important aspects in the gender identity dialogue. Gender identification and expression can be extremely personal and sensitive aspects for each individual. In this context, ensuring privacy and information security for people expressing non-traditional gender identities becomes an additional importance.

The study includes an analysis of current methods and practices of ensuring information security for gender diverse individuals, as well as legal and ethical aspects related to this topic. It also examines ways to protect privacy and personal data in this context and the importance of supporting gender diverse individuals in addressing these issues.

Keywords: information security, gender, gender identity.

Захист приватності та інформаційна безпека завжди були актуальними аспектами сучасного життя, але з розвитком цифрових технологій і збільшенням онлайн-активностей ці питання стали ще більш важливими і складними. Важливо визнати, що існують різні аспекти інформаційної безпеки, які можуть впливати на різні соціальні групи, включаючи гендерну ідентичність. У цьому контексті гендерна ідентичність визначається як особиста ідентичність, пов'язана зі статевими ролями та статевою самоідентифікацією, і може включати трансгендерних, нетрадиційних та гендерно-різних осіб.

Гендерна ідентичність – це особиста ідентичність, яка не завжди співпадає з біологічною статтю. Ця ідентичність може бути трансгендерною,

гендерно-різною, нетрадиційною або відмінною від статевих ролей, які суспільство традиційно пов'язує з чоловічістю або жіночістю. Гендерна різноманітність включає в себе багато різних ідентичностей та виражень, і вона дуже особиста для кожної людини.

Рисунок 1 – Виклики щодо приватності та інформаційної безпеки

Виклики щодо приватності та інформаційної безпеки (рисунок 1):

1.**Кібербулінг і онлайн-дискримінація:**

– Гендерно-різні та трансгендерні особи часто стикаються з онлайн-атаками, включаючи образи, загрози та інші форми кібербулінгу. Важливо розробляти політики та інструменти для виявлення та заборони таких вчинків в соціальних мережах і онлайн-спільнотах.

1.**Приватність та конфіденційність особистої інформації:**

– Особиста інформація, така як ім'я, адреса, статева ідентичність і медична інформація, може бути особливо чутливою для гендерно-різних та трансгендерних осіб. Організації та платформи повинні забезпечувати безпеку цих даних і розробляти політики конфіденційності, які дозволяють особам вибирати, яку інформацію вони хочуть розкрити.

2.**Законодавчий захист:**

– Законодавство повинно гарантувати права та захист гендерно-різних і трансгендерних осіб від дискримінації та порушень приватності. Це може включати в себе створення антидискримінаційних законів та захист від недобросовісної обробки особистих даних.

3.**Технічні засоби безпеки:**

– Важливо підкреслити важливість технічних засобів безпеки, таких як сильні паролі, подвійна аутентифікація та шифрування, для захисту особистої інформації в онлайн-середовищі.

4.**Освіта та свідомість:**

– Надання освіти та підвищення свідомості щодо проблем гендерної ідентичності та приватності важливо як для громадян, так і для фахівців у галузі інформаційної безпеки. Це допомагає зменшити стереотипи і підвищити рівень підтримки.

5. **Захист від дискримінації:**

– Гендерно-різні і трансгендерні особи мають право на захист від дискримінації на основі їхньої гендерної ідентичності. Організації та правоохоронні органи повинні сприяти і виконувати закони, що гарантують це право.

Захист приватності та інформаційна безпека в контексті гендерної ідентичності мають істотне значення для забезпечення рівних прав та справедливості для всіх громадян. Розуміння та урахування особливостей гендерної ідентичності в сфері інформаційної безпеки є ключовим кроком у створенні більш інклюзивного та справедливого суспільства.

Гендерна різноманітність, важлива складова культурного та суспільного розвитку, і всі громадяни мають право на повагу, безпеку та конфіденційність своєї гендерної ідентичності. Однак, як показано в даній темі, особи з нетрадиційною гендерною ідентичністю стикаються з унікальними викликами, пов'язаними зі своєю безпекою та приватністю, особливо в онлайн-середовищі.

Забезпечення безпеки та захисту приватності цих осіб вимагає:

– **законодавчого захисту,** а саме розвиток та прийняття законодавства, яке гарантує права гендерної різноманітності та запобігає дискримінації на основі гендерної ідентичності.

– **технологічних рішень,** розробка та впровадження технічних засобів безпеки, які дозволяють захищати особисті дані та інформацію осіб з нетрадиційною гендерною ідентичністю.

– **свідомості та освіти,** підвищення освіти та свідомості серед суспільства та професіоналів щодо проблем гендерної різноманітності та інформаційної безпеки.

– **активної підтримки, с**творення підтримуючого та невідкладного середовища для осіб з гендерною ідентичністю, яка відрізняється від традиційних статевих ролей.

Захист приватності та інформаційна безпека в контексті гендерної ідентичності – це справедливість, права людини і важливий аспект визнання та поваги до індивідуальної самоідентифікації. Ця тема вимагає спільних зусиль суспільства, законодавців та технологічних галузей для створення більш інклюзивного та справедливого світу для всіх.

Література

1.Механізм забезпечення принципу гендерної рівності: теорія та практика: монографія. — К.: «Хай-Тек Прес», 2018. — 560 с.

УДК 355.58

ГЕНДЕРНІ ВІДМІННОСТІ У СПРИЙНЯТТІ ТА ПОВЕДІНЦІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Гриньова Альона
Львівський державний університет безпеки життєдіяльності, м.Львів

Анотація: Інформаційна безпека є загальною проблемою для всіх користувачів комп'ютерів, незалежно від соціального статусу. Хоча гендерні відмінності в застосуванні технологій досліджені, мало уваги приділено вивченню гендерних відмінностей в інформаційній безпеці. Зростання процесів масової інформатизації показує необхідність комплексного дослідження гендерних аспектів в інформаційному суспільстві. Це передбачає аналіз основних тенденцій, що впливають на становище жінок у сучасному світі. Гендерний підхід до дослідження інформаційного суспільства є новою актуальною проблемою, яка потребує наукового аналізу соціальних явищ та процесів.

Ключові слова: інформатизація, інформаційне суспільство, інформаційно-кому- нікаційні технології (ІКТ), гендер, гендерні проблеми, гендерна нерівність, цифрова нерівність, гендерний розрив, інформаційна безпека, стать, людський фактор, безпекова поведінка.

Abstract: Information security is a common concern for all computer users, regardless of social status. Although gender differences in technology adoption have been explored, little attention has been paid to the study of gender differences in information security. The growth of mass informatization processes shows the need for a comprehensive study of gender aspects in the information society. This involves an analysis of the main trends affecting the position of women in the modern world. The gender approach to information society research is a new, urgent problem that requires a scientific analysis of social phenomena and processes.

Keywords: informatization, information society, information and communication technologies (ICT), gender, gender issues, gender inequality, digital inequality, gender gap, information security, gender, human factor, safety behavior.

Еволюція інформаційних технологій є постійним процесом і невід'ємною частиною нашого повсякденного життя. В кожному будинку присутня принаймні одна з цих технологій - комп'ютери, мобільні телефони, планшети, ноутбуки, ігрові консолі, смарт-телевізори та Інтернет речей, кожна з них має свою операційну систему та широкий набір онлайн-додатків. Розвиток технологій та платформ також ставить перед користувачем завдання розуміння, як правильно використовувати та керувати безпекою в різних технологіях, операційних системах та програмах. Різні фактори, такі як вік, освіта, вік і стать, можуть впливати на спроможність керувати інформаційною безпекою та розуміння її принципів. ITU стверджує, що кількість користувачів Інтернету у світі зросла за останні 10 років більш ніж удвічі — з 2,18 млрд. до 4,95 млрд. За останні 12 місяців кількість користувачів інтернету збільшилася на 192 мільйони людей [1].

Гендер у сфері інформаційної безпеки включає різноманітність статей та ідентифікаційних ознак осіб, які працюють у цій галузі. Хоча інформаційна безпека традиційно була чоловічою доменою, останнім часом спостерігається зростання участі жінок у цьому секторі. За останні роки спостерігається збільшення кількості жінок, які обирають кар'єру в галузі інформаційної безпеки. Жінки займають посади в різних сферах, таких як кібербезпека, захист даних, аналітика загроз, розробка програмного забезпечення та інші. Але незважаючи на це, жінки все ще становлять менший відсоток працівників інформаційної безпеки, ніж чоловіки. Це може бути пов’язано зі стереотипами, які існують щодо ролі жінок у технологічній індустрії, а також з відсутністю належної підтримки та розуміння їхніх потреб у цьому секторі. Для досягнення гендерної рівності у сфері інформаційної безпеки необхідно створити сприятливе середовище для жінок, забезпечити їм доступ до освіти та професійного розвитку, заохочувати їх участь у керівних посадах. Наприклад, деякі суспільства можуть вважати, що жінки повинні займатися домашніми справами і не повинні витрачати час на вивчення технологій. Тому, важливо змінити стереотипи та забезпечити рівні можливості та права для всіх працівників, незалежно від статі. Загалом, забезпечення гендерної рівності та вирішення цифрової нерівності є важливими завданнями для суспільства. Це допоможе забезпечити всім людям рівні можливості та доступ до інформаційних технологій, що є ключовим для сталого розвитку і прогресу.

Як правило, виділяють сім чинників, що лежать в основі цифрової нерівності взагалі: соціальну та національну належність, стать, вік, рівень освіти, мову та географічну зону. Звичайно усі ці чинники між собою взаємопов’язані. Так, гендерний чинник пов’язаний з мовним, тому що значно менша кількість жінок у світі в цілому знають англійську, а більша частка світових веб-ресурсів представлена саме цією мовою.

Результати деяких робіт і експериментів свідчать про значні відмінності між чоловіками та жінками для трьох із шести індивідуальних моделей поведінки у сфері безпеки, і що загальний рівень безпекової поведінки був значно нижчим у жінок, ніж у чоловіків. З точки зору сприйняття безпеки, було виявлено, що жінки також частіше сприймають вищий рівень серйозності загроз безпеці, ніж чоловіки, але сприймають свою вразливість як нижчу – що, можливо, сприяє нижчій загальній поведінці безпеки, що спостерігається [2].

Для зменшення цифрової нерівності необхідно прийняти кілька заходів. По-перше, потрібно забезпечити доступ до освіти з питань ІКТ для жінок. Це може включати створення спеціальних програм і курсів, які спрямовані на жінок і надають їм необхідні навички і знання. Крім того, важливо змінити стереотипи і норми, що обмежують можливості жінок у сфері технологій. Це може бути досягнуто шляхом підтримки ініціатив, які пропагують рівність статей і стимулюють жінок до вивчення і використання ІКТ.

Також важливо забезпечити доступ до інфраструктури ІКТ для всіх соціальних груп. Це може включати розширення мережі Інтернету, будівництво інформаційних центрів та надання доступу до комп'ютерів та інших технологій. Крім того, необхідно забезпечити доступні та якісні послуги ІКТ, які враховують потреби різних соціальних груп.

Проведений аналіз цифрової нерівності показує, що, як правило, до основних гендерних детермінант інформаційного суспільства в українському контексті належать:

- соціально-культурні бар'єри, що ускладнюють безпосередній доступ жінок та ефективне використання ними ІКТ;
- гендерні аспекти науково-технічної освіти та професійного підготування і оволодіння навичками користування ІКТ;
- гендерні аспекти мови ІКТ та гендерний вимір Інтернет-контенту як відображення потреби жінок систематизувати свої знання і виробляти свої погляди, а також мати можливості виразити себе та свої погляди в інформаційному просторі мережі;
- гендерна нерівність в економічній сфері (вартість підключення до мережі, придбання програмного забезпечення, мобільність, права інтелектуальної власності та традиційні жіночі галузі знання);
- відсутність жінок у структурах, відповідальних за прийняття рішень у сфері ІКТ на різних державних рівнях;
- гендерні аспекти політики у сфері ІКТ [3, с. 4].

Загалом, зменшення цифрової нерівності вимагає комплексного підходу, який враховує соціальні, економічні та культурні чинники. Це важливе завдання для суспільства, оскільки цифрова нерівність може призводити до подальшого відставання окремих груп населення і обмежувати їх можливості для розвитку та прогресу. Тому для просування гендерної рівності в сфері інформаційної безпеки необхідно створити сприятливе середовище для жінок, забезпечити їм доступ до освіти та професійного розвитку, а також сприяти їх участі в лідерських ролях. Додатково, важливо змінити стереотипи та впевнитися, що всі працівники мають рівні можливості та права незалежно від своєї статі.

Література

1. Інтернет-ресурс. URL: https://zhuk.ua/istoriyi-ta-fakty/tendentsii-vikoristannya-internetu-u-sviti/

2. Назаденко, Ксенія Сергіївна. Висвітлення гендерних конфліктів у засобах масової комунікації. MS thesis. Київ, 2020.

3. Горошко, О. І. Цифрова нерівність: гендерний аналіз (глобальна і локальна перспективи / О. І. Горошко // Вісн. Міжнар. Слов'ян. ун-ту. Сер.: «Соціологічні науки» – Х., 2008. – Т. XI, № 2. – С. 3– 7.

УДК 004.056

ВИЯВЛЕННЯ, АНАЛІЗ ТА ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ З ВИКОРИСТАННЯМ SECURITY OPERATIONS CENTER

Гриченко Даниїл, Андрій Лагун
Львівський державний університет безпеки життєдіяльності

Security Operation Center (SOC) є ключовим елементом кібербезпеки. Розглядається роль SOC у виявленні, аналізі та запобіганні кіберзагрозам, надаючи уявлення про ефективні стратегії захисту для організацій у сучасному цифровому середовищі.

Ключові слова: SOC (Security Operation Center), роль SOC у виявленні загроз, ефективні стратегії захисту.

Security Operation Center (SOC) is a key element of cyber security. Was considered the SOC's role in detecting, analyzing and preventing cyber threats, providing the identification of effective strategies to protect organizations in today's digital environment.

Keywords: SOC (Security Operation Center), the role of SOC in threat detection, effective protection strategies.

В наші дні, коли кіберзагрози стають все більш складними та вдосконаленими, Security Operations Center (SOC) стає важливішим захисником сучасних організацій. Досліджуючи роль SOC та його ключові компоненти: аналітиків та інтелектуальні системи. Розкривається, як ці фактори спільно працюють для виявлення, аналізу та запобігання кіберзагрозам, забезпечуючи безпеку в цифровому світі.

Звісно ж, Security Operations Centers (SOC) є невід'ємною частиною кібербезпекової стратегії різних організацій, незалежно від їхнього розміру чи галузі. У сучасному цифровому світі загрози можуть дістати будь-яку компанію, іноді навіть тих, хто вважає себе надійно захищеним. Ідея, що "всіх можуть взломати", вже стала стандартом у кібербезпеці. Тут питання полягає не в тому, чи буде вас взламано, а коли це станеться і наскільки ефективно ви зможете реагувати.

SOC надає можливість виявляти та запобігати кіберзагрозам у реальному часі. Це дозволяє організаціям оперативно реагувати на інциденти та запобігати можливим збиткам. Незалежно від обсягу ресурсів, часу чи фінансів, які ви готові вкласти в кібербезпеку, SOC може адаптуватися до ваших потреб та можливостей. Він забезпечує не лише захист від потенційних загроз, але і визначену реакцію та готовність до інцидентів, забезпечуючи надійність у сфері кібербезпеки будь-якої організації.

Також, SOC-команда стикається із рядом викликів, включаючи постійні зміни в кіберзагрозах, великий обсяг даних та логів, потребу реагування в реальному часі, вдосконалення технологій та шифрування, брак кваліфікованих фахівців, необхідність співпраці з іншими відділами та відповідність законодавчим вимогам. Розв'язання цих викликів вимагає

технічних знань, співпраці та постійного вдосконалення навичок з боку SOC-команди.

Важливо відзначити, що забезпечення кібербезпеки організації вимагає ефективної взаємодії між аналітиками різних рівнів в SOC-команді. Tier 1 аналітики виявляють базові загрози та передають більш складні випадки Tier 2, які співпрацюють з висококваліфікованими Tier 3 аналітиками для аналізу найскладніших сценаріїв. Ця взаємодія дозволяє швидко та ефективно виявляти, аналізувати та реагувати на різноманітні кіберзагрози, забезпечуючи надійний захист організації від кібернебезпеки.

Особливо важливою частиною команди є SOC інженери, які відіграють ключову роль у команді кібербезпеки. Вони є основними архітекторами та супровідниками технічних інструментів, таких як SIEM системи та системи виявлення вторгнень. Ці інженери розробляють і вдосконалюють політики безпеки, забезпечуючи надійність захисту організації в цифровому просторі. Вони є невід'ємними та ключовими учасниками команди, відіграючи важливу роль у виявленні та запобіганні кіберзагрозам.

SOC команда забезпечує ефективну комунікацію з клієнтом під час кібератак за допомогою чітких та зрозумілих повідомлень. Швидка реакція, постійний зворотний зв'язок та емпатія в комунікації є ключовими аспектами. Крім того, команда розробляє план відновлення разом з клієнтом, надає конкретні рекомендації з покращення кіберзахисту та забезпечує професіоналізм та відзначену емпатією комунікацію, сприяючи успішному управлінню атакою та відновленню безпеки системи.

Слід відмітити, що комунікація з клієнтами є індивідуальним та унікальним процесом для кожної організації. Наприклад, деякі компанії можуть демонструвати затримку у відгуках на активність SOC команди через власні внутрішні політики або процедури. Також, у деяких випадках, працівники компанії можуть бути недоступні або відпочивати, що може сповільнити обмін інформацією під час кібератаки. Це підкреслює важливість терпіння та гнучкості з боку SOC команди, яка повинна адаптуватися до різних графіків та вимог клієнтів для ефективної комунікації та реагування на кіберзагрози.

Проактивність SOC-команди виявляється у виявленні можливих кіберзагроз перед їхньою активізацією. Аналізуючи аномалії та використовуючи Threat Intelligence, застосовується методика створення сценаріїв можливих атак для ефективного уникнення потенційних загроз у цифровому просторі.

Особливо важливою частиною роботи Security Operations Center (SOC) є його проактивна діяльність у виявленні та запобіганні кіберзагрозам. У світі постійних технологічних вдосконалень і зростаючих кількості кіберзагроз, SOC-команди відіграють ключову роль у забезпеченні безпеки організацій. Їхня робота полягає не лише у реакції на вже виниклі загрози, але й у передбаченні та запобіганні майбутнім інцидентам.

Проактивність SOC-команди визначається її здатністю аналізувати та розуміти не тільки вже існуючі методи атак, але й передбачати нові загрози, які можуть виникнути в майбутньому. Це означає постійний моніторинг мережі, виявлення аномалій та розробку стратегій для запобігання можливим атакам, перш ніж вони набувають сили.

У наш час, коли кіберзагрози стають все більш витонченими та складними, проактивна діяльність SOC-команди є невід'ємною складовою ефективної кібербезпеки. Їхні навички та знання допомагають уникати серйозних загроз для організацій та забезпечують безпеку в цифровому світі.

Створення ефективного Security Operations Center (SOC) розпочинається з розробки чіткої стратегії, яка відповідає бізнес-цілям організації. Це включає оцінку масштабів підприємства, інвентаризацію активів і вразливих місць, а також розробку ефективних процесів моніторингу, виявлення та реагування на загрози. З огляду на постійно зростаючу складність загроз, організаціям важливо постійно оновлювати свою стратегію, звертаючи увагу на нові ризики, і вивчати найкращі практики для збереження бізнес-продуктивності.

SOC - це комплексне поєднання людей, процесів і технологій, яке забезпечує безпеку організації в цифровому світі. Важливі компоненти SOC включають SIEM для збору та аналізу даних, цифрові системи моніторингу для виявлення аномалій, засоби запобігання (брандмауери, антивірусне ПЗ), інструменти виявлення загроз, що використовують штучний інтелект, та автоматизовані можливості реагування. Використання передових хмарних рішень безпеки, наприклад CrowdStrike Falcon, допомагає ефективно боротися з сучасними кіберзагрозами та забезпечує безпеку активів організації в режимі реального часу.

Отож, в сучасному цифровому світі, де кіберзагрози стають все більш складними і небезпечними, існення Security Operations Center (SOC) стає невід'ємною частиною життя будь-якої організації. SOC відіграє ключову роль у виявленні, аналізі та запобіганні кіберзагрозам, забезпечуючи надійний захист та безпеку в цифровому просторі.

Література

1. https://underdefense.com/services/incident-response/
2. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
3. https://www.rapid7.com/blog/post/2016/06/07/how-to-structure-a-security-operations-center/
4. https://www.crowdstrike.com/cybersecurity-101/security-operations-center-soc/
5. https://istrosec.com/blog/threat-intel-with-soc/
6. https://www.crowdstrike.com/cybersecurity-101/security-operations-center-soc/best-practices/

УДК 004.056.5:005.8

СИСТЕМА ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Дальовський Р. Я., Головатий Р.Р.
Львівський державний університет безпеки життєдіяльності, м. Львів

Висвітлено основи захисту інформації у комп'ютерних системах від несанкціонованого доступу. Розглянуті головні фактори, які необхідно врахувати при проектуванні безпечної мережі. Проаналізовано найпоширеніші методи Інтернет-атак та інших загроз в сучасних комп'ютерних мережах.

Ключові слова: аспекти безпеки, Інтернет-атака, Інтернет-протокол, комп'ютерна мережа, криптографічні системи, мережева безпека, програмного забезпечення мережевої безпеки, система виявлень вторгнень.

The basics of information protection in computer systems from unauthorized access are highlighted. The main factors necessary to consider in designing a secure network are discussed. The most prevalent methods of Internet attacks and other threats in modern computer networks are analyzed.

***Keywords*:** security aspects, Internet attack, Internet protocol, computer network, cryptographic systems, network security, network security software, intrusion detection system.

Задача захисту інформації в комп'ютерних системах на сьогоднішній день є актуальною внаслідок широкої розповсюдженості таких систем, розширення комп'ютерних мереж, якими передаються великі обсяги інформації. Забезпечення безпечної діяльності комп'ютерних систем необхідне для будь-яких підприємств і установ, починаючи від державних організацій і закінчуючи невеликими приватними фірмами, незалежно від виду їх діяльності. Інтернет класифікується як мережа передачі даних.

Оскільки поточна мережа даних складається з комп'ютерних маршрутизаторів, спеціальні про- грами, такі як «троянські коні», закладені в маршрутизатори, можуть отримувати інформацію. Оскільки синхронна мережа, яка складається з комутаторів, не буферизує дані, вона не вразлива для зловмисників. Ось чому мережі передачі даних, такі як Інтер- нет, та інші мережі, які підключаються до Інтернету, надають перевагу безпеці. Розвиток сучасних інформаційних технологій супроводжується збільшенням ролі телекомунікаційних систем різного призначення та комп'ютерних мереж. Це пояснюється необхідністю більш швидкої передачі інформації, в тому числі й управлінської, для якої важливе значення мають час та оперативність її доставки до користувачів.

Більш вагомим стає використання засобів електронного обміну документів – електронної пошти, програмного забезпечення браузерів тощо – за допомогою яких набагато збільшується ефективність роботи фахівців різних

рівнів управління сучасними підприємствами та установами. На сьогодні мережева безпека це великий набір вимог та політик, які пред'являються до мережевої корпоративної інфраструктури для аналізу її роботи та недопущення доступу до даних зловмисників, зміни цих даних, їх модифікації.

Мережеві (Network-based IDS, NIDS) контролюють пакети в мережевому оточенні і виявляють спроби зловмисника проникнути всередину системи або реалізувати атаку «відмова в обслуговуванні». Ці IDS працюють з мережевими потоками даних. Типовий приклад NIDS – система, яка контролює велике число TPC-запитів на з'єднання (SYN) з багатьма портами на обраному комп'ютері, виявляючи, таким чином, що хтось намагається здійснити сканування TCP портів. Мережева IDS може запускатися або на окремому комп'ютері, який контролює свій власний трафік, або на виділеному комп'ютері, прозоро переглядають весь трафік у мережі (концентратор, маршрутизатор). Мережеві IDS контролюють багато комп'ютерів, тоді як інші IDS контролюють тільки один. Прикладом мережевої IDS є Snort. IDS, які встановлюються на хості і виявляють зловмисні дії на ньому називаються хостовими або системними IDS.

Прикладами хостових IDS можуть бути системи контролю цілісності файлів, які перевіряють системні файли з метою визначення, коли в них були внесені зміни. Монітори реєстраційних файлів, контролюють реєстраційні файли, створювані мережевими сервісами і службами. Обманні системи, що працюють з псевдосервісами, мета яких полягає у відтворенні добре відомих вразливостей для обману зловмисників.

Найближчим часом поєднання протоколу IPv6 та елементів безпеки, такі заходи, як брандмауери, виявлення вторгнень та процедури аутентифікації будуть успішними для захисту мереж.

Застосування інформаційних технологій (IT) вимагає підвищеної уваги до питань інформаційної безпеки. Руйнування інформаційного ресурсу, його тимчасова недоступність або несанкціоноване використання можуть завдати значних матеріальних збитків. Без належної ступеня захисту інформації впровадження IT може виявитися економічно невигідним в результаті значних втрат конфіденційних даних, що зберігаються і обробляються в комп'ютерних мережах. Реалізація рішень, що забезпечують безпеку інформаційних ресурсів, істотно підвищує ефективність всього процесу інформатизації в організації, забезпечуючи цілісність, справжність і конфіденційність дорогої інформації, що циркулює в локальних і глобальної інформаційних середовищах.

Слідом за масовим застосуванням сучасних інформаційних технологій криптографія вторгається в життя сучасної людини. На криптографічних методах засноване застосування електронних платежів, можливість передачі секретної інформації по відкритих мережах зв'язку, а також вирішення великого числа інших завдань захисту інформації в комп'ютерних

системах та інформаційних мережах. Потреби практики призвели до необхідності масового застосування криптографічних методів, а отже до необхідності розширення відкритих досліджень та розробок у цій області. Володіння основами криптографії стає важливим для вчених і інженерів, що спеціалізуються в області розробки сучасних засобів захисту інформації, а також в областях експлуатації та проектування інформаційних та телекомунікаційних систем.

Безпека мережі є важливою сферою, яка набирає обертів, оскільки Інтернет-атаки та інші різновиди загроз зростають в геометричних розмірах. Щоб оцінити необхідні зміни в техніці систем безпеки комп'ютерних мереж, були проаналізовані загрози безпеки та Інтернет-протокол. Більшість технологій безпеки базується на програмному забезпеченні, але на даний час маємо необхідно додатково використовувати апаратні засоби систем захисту.

Література

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков – К.: Видавнича група BHV, 2009. – 608 с.

2. Bound (ed.), "IPv6 Enterprise Network Scenarios". IETF Internet Draft. July 2004.

3. Durand, S. Roy, and J. Paugh, "Issues with Dual Stack IPv6 on by Default". IETF Internet Draft. July 2004.

4. Михайлюта С. Л., Степанушко І. В., Бабич Б. О., Ткаченко В. Ю., Лавринович В. С. Дослідження мережевих DOS-атак, що ґрунтуються на використанні протоколу ICMP // Вісник Інженерної академії України. - К.: 2009. – № 2. – С. 146–149.

5. Вертузаєв М. С., Юрченко О. М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник / За ред. С. Г. Лаптєва,— К.: Вид-во Європ. ун-ту, 2001.— 321 с.

УДК 004.932.2

СТЕГАНОЗАХИСТ АУДІСИГНАЛІВ НА ОСНОВІ СИНГУЛЯРНОГО РОЗКЛАДУ МАТРИЧНОГО ОПЕРАТОРА

Дмишко Ю.Г., Пелешко Д.Д., Винокурова О.А.
Львівський національний університет імені Івана Франка

Анотація. Дослідження присвячене модифікації стеганографічного алгоритму на основі сингулярного розкладу для приховування інформації в аудіосигналах. Розглянуто методи конвертації сегментів аудіо сигналу в матричний оператор та основні етапи розробки стеганографічного програмного забезпечення. Показано, розроблене програмне забезпечення для стеганографії в аудіофайлах є ефективним з точки інвізібільності вбудовування секрету в аудіо.

Ключові слова: стеганографія, сингулярний розклад, аудіосигнали, методи маскування даних, стійкість до стиснення.

Abstract. The study is devoted to the modification of the steganographic algorithm based on the singular value decomposition for hiding information in audio signals. The methods of converting an audio signal into a matrix are considered. It is proved that software for steganography in audio files requires the integration of efficient algorithms and ensuring resistance to various attacks.

Keywords: steganography, singular value decomposition, audio signals, data masking methods, compression resistance.

Проблема маркування даних з точки зору забезпечення збереження авторських прав, секретної передачі даних, тому числі і цифрових звукових сигналів на сьогодні є актуальною. Особливо у випадках використання відкритих джерел інформації чи комунікаційних каналів. У відповідь на цей виклик, стеганографія пропонує рішення, що базується на ефективних методах перетворення аудіосигналів для приховування інформації [1].

Ефективна стеганографія у аудіофайлах вимагає складних та точних методів перетворення аудіосигналів. Ми у своїй роботі для стеганозахисту пропонуємо використовувати алгебраїчні розклади квадратних матриць.

Розглянемо три основні методи конвертації сегментів аудіо сигналу в матрицю, кожен з яких має свої унікальні властивості та застосування у стеганографії.

Діагональний метод. Принцип роботи- аудіосигнал поділяється на рівні частини, кожна з яких розміщується вздовж діагоналі матриці. Перевагами такого методу є рівномірний розподіл даних. Це знижує ймовірність виявлення прихованої інформації. Проте стеганозахист на основі цього підходу є більш складний у реалізації і може вимагати додаткових ресурсів для обробки.

Горизонтальний метод. Принцип роботи є таким - дані розміщуються у послідовних рядках матриці. Це суттєво спрощує обробку. А сам метод вимагає менше часу на обробку та є менш стійким до методів стеганоаналізу.

Вертикальний метод. Принцип роботи - фрагменти аудіо розміщуються у стовпцях матриці. Даний метод може бути ефективнішим у приховуванні даних у певних типах аудіосигналів і є складнішим у реалізації та може вимагати більше обчислювальних ресурсів [2].

Зауважимо, що кожен метод має свої специфічні сценарії застосування. Наприклад, діагональний метод може бути вигідним у ситуаціях, де потрібна висока стійкість до виявлення, тоді як горизонтальний метод може бути кращим у випадках, коли потрібна швидка обробка. Важливо враховувати ці особливості при виборі методу конвертації.

Розробка програмного забезпечення для стеганографії в аудіофайлах вимагає інтеграції ефективних алгоритмів і забезпечення стійкості до різних атак.

Розглянемо етапи розробки такого програмного забезпечення.

Етап 1. Огляд основних технічних та функціональних вимог до програмного забезпечення, включаючи інтерфейс користувача, способи обробки аудіо, стеганографічні алгоритми.

Етап 2. Детальний опис архітектури розробленого програмного забезпечення, включаючи модулі обробки аудіо, вбудовування та вилучення інформації, а також механізми безпеки [4].

Етап 3. Глибокий аналіз алгоритму сингулярного розкладу, його переваги у контексті стеганографії та інтеграція в програмне забезпечення.

Етап 4. Опис інтуїтивно зрозумілого користувацького інтерфейсу, що дозволяє легко вбудовувати та вилучати інформацію.

Етап 5. Розгляд функцій програми, включаючи формати аудіофайлів, що підтримуються, налаштування параметрів стеганографії та можливості зворотного відтворення.

Етап 6. Опис підходів до тестування, включаючи модульне тестування, інтеграційне тестування та тестування використання.

Етап 7. Аналіз результатів тестування з акцентом на ефективність вбудовування, точність вилучення та стійкість до стеганоаналізу.

Етап 8. Обговорення проведених випробувань програми на стійкість до різних видів атак, включаючи стиснення аудіо, шум, фільтрацію [5].

Етап 9. Порівняння розробленого програмного забезпечення з іншими відомими стеганографічними рішеннями, включаючи оцінку ефективності, зручності використання та безпеки.

Висновки. Аналіз літературних джерел показав важливість розробки ефективного стеганографічного алгоритму для практичних задач маркування аудіосигналів. Це підтверджує актуальність проведених досліджень і розробки та практичної реалізації методу заснованого на сингулярному розкладі.

Ефективне використання діагонального, горизонтального та вертикального методів конвертації аудіосигналів у матрицю забезпечує гнучкість та покращує ефективність стеганографії, а програмне забезпечення враховує важливі аспекти безпеки та стійкості, інтегруючи сингулярний розклад для оптимізації процесу стеганографії. Використання сингулярного розкладу значно підвищує ефективність та надійність стеганографії, особливо у контексті невидимості секрету та стійкості до різних атак [6]. Методи конвертації дозволяють ефективно обробляти аудіосигнали, забезпечуючи баланс між швидкістю обробки та стійкістю до виявлення. Програмне забезпечення може бути ефективно використане для захисту інформації в комерційних та особистих цілях, особливо в умовах, де потрібна висока конфіденційність.

Подальші дослідження можуть бути спрямовані на покращення алгоритмів та розширення функціональності програмного забезпечення для забезпечення ще більшої ефективності та стійкості.

Література

1. Іванов В.Г. Захист інформації засобами комп’ютерної стеганографії. Безпекове інноваційне суспільство: взаємодія у сфері правової освіти та правового виховання: матеріали міжнар. інтернет-конф, 2016. С.53-56.

2. Бендер, В., Груль, Д., Морімото, Н.: Методи приховування даних. IBM Systems Журнал 35(3), 313-336 (1996)

3. Венката Сайманой, І.: Криптографія та стеганографія. Міжнародний журнал комп'ютерних застосувань (0975 - 8887) 1(12), 63-68 (2010)

4. Використання методу фазового кодування для приховування конфіденційної інформації в аудіофайлах. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/758/1/19.pdf

5. Джонсон, М., Ішвар, П., Прабхакаран, В.М., Шонберг, Д., Рамчандран, К.: Про стиснення зашифрованих даних. IEEE Trans. on Signal Processing 51, 2992- 3006 (2004) Deepsound. uptodonw. URL: https://deepsound.ru.uptodown.com/windows

6. Ендрюс, Г.К., Паттерсон, К.Л.: Кодування зображень методом сингулярного розкладання (SVD). IEEE Trans. on Communications 24(4), 425-432 (2002)

УДК 004.056

КОМПЛЕКСНА МОДЕЛЬ БЕЗПЕКИ ІНТЕЛЕКТУАЛЬНОЇ КІБЕРФІЗИЧНОЇ ТРАНСПОРТНОЇ СИСТЕМИ

Дудикевич В.Б., Микитин Г.В., Кутень Р.Б., Сидорик Д.О.
Національний університет "Львівська політехніка", Львів

Анотація. У просторі задач безпечної інтелектуалізації запропоновано структуру багаторівневої безпеки кіберфізичної системи (КФС) "Інтелектуальна транспортна система"("ІТС") на основі методики загроз STRIDE Розроблено програмну реалізацію захищеного обміну інформацією в комунікаційному середовищі КФС "ІТС" згідно моделі OSI на основі алгоритму "Калина" засобами мови програмування C#.

Вступ. За векторами Концепції Індустрії 4.0 і Стратегії кібербезпеки сьогодні триває безпечна інтелектуалізація інфраструктури в Україні, що зокрема розгортає впровадження технологій підтримки функціонування ІТС – безпечних кіберфізичних систем [1, 2].

Комплексна система безпеки інтелектуальної транспортної системи. Комплексна багаторівнева модель безпеки ІТС (рис. 1) побудована на основі: 1) багаторівневої КФС "фізичний простір (ФП) – комунікаційне середовище (КС) – кібернетичний простір (КС)"; 2) загроз зовнішнього і внутрішнього рівня КФС: моделі загроз STRIDE для ФП; моделі загроз КС згідно OSI; моделі загроз основним профілям безпеки – конфіденційності, цілісності, доступності для КП; 3) технологій безпеки ФП, КС, КП зовнішнього і внутрішнього рівнів; 4)мандатної політики безпеки.

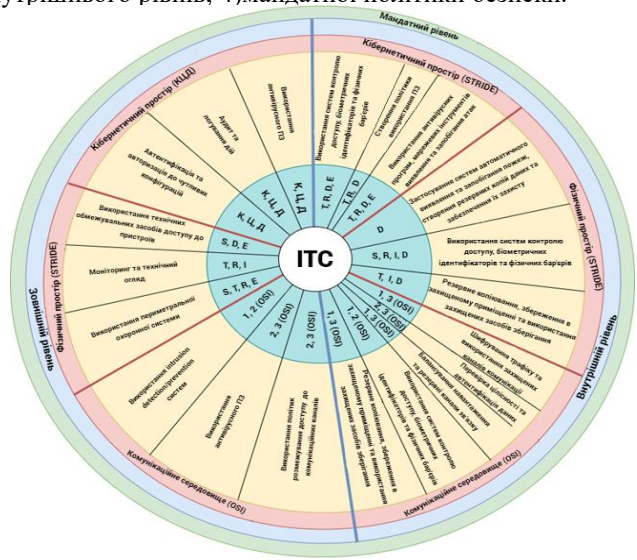


Рисунок 1 – Структура комплексна багаторіневої моделі безпеки КФС "ІТС"

Захищений канал комунікаційного середовища ІТС: програмна реалізація алгоритму шифрування даних на основі алгоритму "Калина" та мови C#. Для програмної реалізації алгоритму "Калина" використана мова програмування C#, швидкодія та кросплатформеність якої дозволить використовувати програму на будь-якому пристрої для захисту інформації в технологіях безпровідного зв'язку. Розміри ключа та блоку становлять 512 біт, що забезпечує максимальний рівень криптостійкості. На рис. 2. та 3. наведені блок-схеми роботи програми шифрування даних та генерації раундових ключів відповідно.

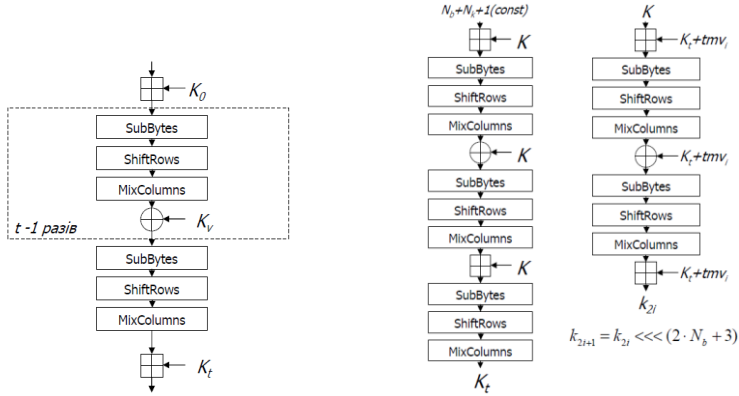


Рисунок 2 – Криптографічний захист даних в комунікаційному середовищі КФС "ІТС":
а) алгоритм шифрування "Калина"; б) блок-схема генерації раундових ключів

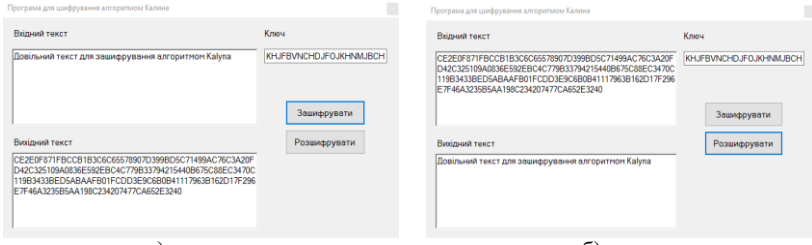


Рисунок 3 – Результат програмної реалізації захищеного обміну інформації:
а) шифрування; б) дешифрування

Література

1. Yurchak Oleksandr. "Ukrayins'ka stratehiya Industriyi 4.0 – 7 napryamiv rozvytku" [Електронний ресурс] – Режим доступу: https://industry4-0-ukraine.com.ua/2019/01/02/ukrainska-strategiya-industrii-4-0-7-napriankiv-rozvutku.

2. Стратегія кібербезпеки України. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#n12

УДК 004.056

БЕЗПЕКА ІНФОРМАЦІЙНИХ ПРОЦЕСІВ ЦЕНТРУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ НУ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

Дудикевич В.Б., Микитин Г.В., Лосев З.О.
Національний університет “Львівська політехніка”, Львів

Анотація. Розглянуто структуру інформаційного процесу (ІП) центру інформаційного забезпечення (ЦІЗ) НУ “Львівська політехніка” на рівні: фаз, операцій, обробки інформації. Запропонована комплексна система безпеки ІП на рівні фаз за впливу цілеспрямованих і випадкових загроз.

Вступ. В Україні розгортаються процеси безпечної цифрової трансформації інфраструктури суспільства в рамках цифрової Стратегії ЄС за програмою EU4Digital: Кібербезпека – Схід [1]. Важливим вектором цієї програми є – безпека інформаційних процесів центрів інформаційного забезпечення закладів вищої освіти за ймовірного впливу цілеспрямованих і випадкових загроз.

Інформаційні процеси: загроза – захист. *Інформаційні ресурси* ЦІЗ НУ “Львівська політехніка”, які взаємодіють з інформаційними процесами, – бази даних (БД), бази знань, масиви інформації, сховища даних, бази моделей. *Інформаційні процеси* ЦІЗ – створення, збір, зберігання, обробка, відображення, обмін, розповсюдження й використання інформації. На рис. 1 представлено функціонування інформаційного процесу ЦІЗ НУ “Львівська політехніка” на рівні: фаз, операцій, обробки.

Рисунок 1 – Інформаційні процеси ЦІЗ на рівні: фаз, операцій, обробки

Для БД ЦІЗ особливими є програмні загрози, серед яких: відмова програмного забезпечення; модифікація даних; витік, порушення цілісності, достовірності й збережності інформації при її обробці;“чистка сміття” на диску або в оперативній пам'яті; установка неперевірених виконуваних модулів і командних процедур, де ймовірно можуть знаходитися “троянські коні”, “черв'яки” т.і.. На протидію таким загрозам використовуються програмні засоби захисту: захист паролем; шифрування даних і програм; захист полів та записів таблиць БД; розділення прав доступу до об’єктів БД; забезпечення цілісності зв’язків таблиць; антивірусне програмне забезпечення; цифровий псевдонім; запобігання створення несанкціонованої інформації; управління потоком захищених процедур і програм при передаванні з одного сегмента БД в інший.

Розглянемо комплексну систему безпеки інформаційних процесів ЦІЗ на рівні фаз: сприйняття/ збір / відбір; передавання; обробки; зберігання; представлення/ впливу (табл. 1).

Таблиця 1 – Цілеспрямовані і випадкові загрози безпеці ІП на рівні фаз

Інформаційні процеси	**Загрози**		**Захист інформації**	
Фази	**Цілеспрямовані**	**Випадкові**	**Апаратний**	**Програмний**
1.1. Сприйняття / збір / відбір	порушення конфіденційності інформації; відключення або виведення з ладу підсистем забезпечення функціонування системи	помилки людини, як джерела інформації; людини оператора; неправильні дії обслуговуючого персоналу; помилки людини, як ланки, що приймає рішення	1. Guardant 2. eToken 3. SenseLock 4. HASP	1. ЕЦП 2. StarForce 3. LaserLock 4. Fairplay 5. Adobe Editions
1.2. Передавання	отримання несанкці- онованого віддаленого доступу; затримання передавання повідомлення; фізичне руйнування системи або виведення з ладу найбільш важливих її компонентів	завади в лініях зв’язку від впливів зовнішніх факторів; збої чи нестабільність роботи технічних пристроїв; електромагнітне випромінювання; відмова систем електроживлення	1.Cryptophone G10i 2. Luna SA 3. nShield Connect 4. Бар'єр-301 5. Гряда-301	1. Secret Disk Server NG 2. RedPhone 3. RedPhone Net LSP 4. Secret Pack Rus 5. Thales

1.3. Обробка	вхід в інформаційну систему в обхід засобів захисту; порушення конфіденційності інформації (перехоплення побічних електромагнітних випромінювань); втрата інформації; вірусні атаки	відмови програмного та апаратного забезпечення; збої чи нестабільність роботи технічнихзасобів; стихійні лиха	1. Luna CA4 2. Luna PCI 3.ProtectServer Gold (мініпристрій) 4. KOKON-R	1. TrueCrypt 2. R-Crypto Disk Security 3. Secret Disk Server NG
1.4. Зберігання	злам шифрів криптографічного захисту інформації; фізичне руйнування системи; порушення цілісності та конфіденційності інформації	технічні несправності мережі і компонентів; відмова систем електроживлення; помилки людини	1. М-590 2. Secure IDE 3. РУТОКЕН 4. CryptoLine 358 5. Кристал-1Д	1. BestCrypt Volume Encryption 2. Secret Disk 3. WISeCrypt 4. Crypto Composer
1.5. Представлен-ня / вплив	віддалений запуск додатків; порушення конфіденційності інформації	несанкціонований доступ до адміністративної частини відмова систем електроживлення; помилки операторів	1. Бар'єр-301 2. Luna PCI 3. nShield Solo 4. HASP	1. Secure Pack Rus 2. Fairplay 3. LaserLock

Література

1. Програма EU4Digital: Кібербезпека – Схід. – [Електронний ресурс]. – Режим доступу: https://eufordigital.eu/uk/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/]/

УДК 004.056.5+534.2.001.2

РОЗРОБКА ЗАСОБУ ЗАХИСТУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ВИКОРИСТАННЯ ПОТОКОВОГО АЛГОРИТМУ ШИФРУВАННЯ RC4

Івануса Андрій, Колос Надія, Малькевич Роман, Сахан Петро
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. Запропонована програмна та апаратна архітектура для засобу «прозорого» шифрування даних на з'ємних носіях з використанням поточного алгоритму шифрування RC4. За допомогою мови моделювання UML побудовано ряд діаграм, що формалізують запропоновану архітектуру. На їх основі розроблено працездатний прототип.

Ключові слова: *захист інформації, шифрування, криптографія, алгоритм, RC4.*

Abstract. Proposed software and hardware architecture for a means of "transparent" data encryption on removable media using the current RC4 encryption algorithm. Using the UML modeling language, a number of diagrams formalizing the proposed architecture were constructed. Based on them, a workable prototype was developed.

Keywords: *information security, encryption, cryptography, algorithm, RC4.*

Для зменшення показника вразливості системи від кіберзагроз необхідно впливати на окремі показники. Такий вплив може бути досягнений за допомогою накопичувача даних з "прозорим" шифруванням та відкритою апаратною і програмною архітектурами. Таким чином, потрібно спроектувати і розробити працездатний прототип накопичувача даних з відкритою архітектурою. Користувачами закінченого рішення можуть бути будь-які зацікавлені приватні особи чи організації. Тому метою роботи є розробка архітектури для засобу захисту інформації, а також реалізація його дешевого і працездатного прототипу.

В якості основного критерію класифікації криптографічних алгоритмів використовується тип виконуваного над вихідним текстом перетворення. Класифікацію криптографічних алгоритмів в нотації UML діаграми класів наведено на рисунку 1.

Сьогодні блокові алгоритми, такі як AES, широко використовуються для захисту даних під час їх передачі на великих швидкостях. Інший широко відомий симетричний шифр, Rivest Chiper 4, є менш вимогливим до обсягу оперативної пам'яті та є більш простим для розуміння. Саме цей алгоритм використовується в стандарті WEP для забезпечення захисту передачі даних в реальному часі, тому для створення прототипу захисту інформації автор обрав RC4.

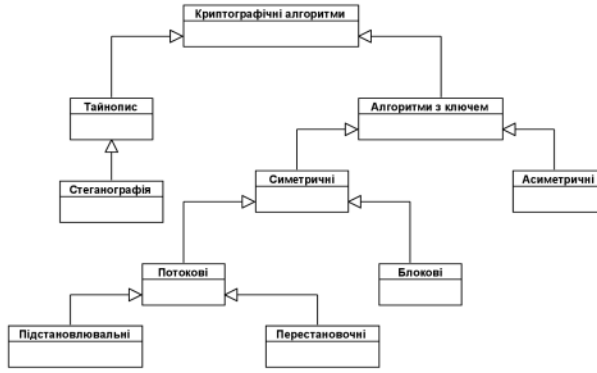


Рисунок 1 – Класифікація криптографічних алгоритмів

Rivest Cipher 4 – потоковий шифр, що широко застосовується в різних системах захисту інформації в комп'ютерних мережах (наприклад, в протоколах SSL і TLS, алгоритмі безпеки бездротових мереж WEP і WPA). На вхід алгоритму RC4 надходить потік даних для шифрування m і послідовність ключових бітів k. Так виходить шифрограма c:

$$c_i = m_i \oplus k_i$$

Розшифровка полягає в регенерації ключового потоку (ki) і складення з шифрограмою (ci) по модулю двох. В силу властивостей підсумовування за модулем двох на виході ми отримаємо вихідний не зашифрований текст (mi):

$$m_i = c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i$$

За умови, що послідовність бітів ключа обирається довільно і не має періодів, зламати шифр неможливо, але виникає проблема передачі довгого ключа. Тому на практиці для генерації ключового потоку k використовується генератор псевдовипадкових чисел на основі заданого ключа. Процес отримання ключового потоку k складається з двох етапів:

1) ініціалізація S-блоку (Key-Scheduling Algorithm);

2) генерація псевдовипадкових чисел ki (Pseudo-Random Generation Algorithm).

Генератор ключового потоку RC4 переставляє значення, що зберігаються в S. В одному циклі RC4 визначається одне n-бітове слово K з ключового потоку. Надалі ключове слово буде складено по модулю два з вихідним текстом, який користувач хоче зашифрувати.

У результаті роботи запропонована програмна та апаратна архітектура для засобу «прозорого» шифрування даних на з'ємних носіях з використанням поточного алгоритму шифрування RC4. За допомогою мови моделювання UML побудовано ряд діаграм, що формалізують запропоновану архітектуру. На їх основі розроблено працездатний прототип.

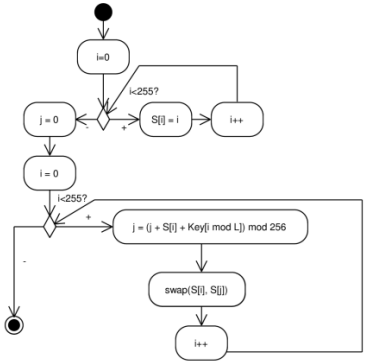


Рисунок 2 – Діаграма діяльності для Key-Scheduling Algorithm

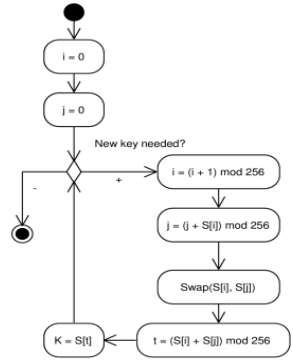


Рисунок 3 – Діаграма діяльності для Pseudo-Random Generation Algorithm

Література

1. Криптографічні та стенографічні засоби захисту інформації. Полотай О.І., Овчиннікова К., Лагун А.Е. Зб. тез доп. IV Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології”. (м. Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 146–148.

2. Neural Network-Based Cryptography: A Primary Study on the Performances and Techniques/ Jia-Lin Foo, Kok-Why Ng, Palanichamy Naveen/ Proceedings of the International Conference on Computer, Information Technology and Intelligent Computing (CITIC 2022). – 2022. – p. 68-78.

3. Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning/Gohr, A. /Advances in Cryptology – CRYPTO 2019. Lecture Notes in Computer Science, vol 11693, – p. 150-179.

4. Yakovchuk R., Kuzyk A., Olexander Kagitin O., Ivanusa A. and Yemelyanenko S. FDS simulation of fire spreading on facade heat insulating system // IOP Conference Series: Earth and Environmental Science, International Conference on Sustainable Future and Environmental Science. – Bucharest, Romania, 2021. – V. 635. – P. 012009.

5. Івануса А. І., Яковчук Р. С., Ємельяненко С. О., Івануса З. З. Управлінські та інформаційні особливості проекту безпечної експлуатації спортивно-видовищних споруд. Науковий вісник НЛТУ України. 2019, т. 29, № 8. С. 134–141.

6. Ivanusa, A., Marych, V., Kobylkin, D., & Yemelyanenko, S. (2023). Construction of a visual model of people’s movement to manage safety when evacuating from a sports infrastructure facility. Eastern-European Journal of Enterprise Technologies, 2(3 (122), 28–41. https://doi.org/10.15587/1729-4061.2023.277492.

7. Ivanusa A. «Project of forming «culture and safety» of the airport» // MATEC Web of Conferences, V. 247, 00045 (2018) https://doi.org/10.1051/matecconf/20182470004.

УДК 004.056.5+534.3.001

ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У ПРОГРАМНИХ ПРОДУКТАХ З ВІДКРИТОЮ АРХІТЕКТУРОЮ

Івануса Андрій, Петрович Андрій, Ткач Мар'ян, Торкотюк Євгеній
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. Для тестування низькорівневого програмного коду розроблена модель мікропрограмного забезпечення, для якої проводиться модульне тестування, та тестування швидкодії. Проведене порівняння швидкодії однакового програмного коду на різних апаратних платформах. Висунуто припущення, що розробка та підтримка моделі мікропрограмного забезпечення в цілях тестування може бути більш доцільною, ніж тестування безпосередньо на пристрої, що розробляється.
Ключові слова: *захист інформації, програмне забезпечення.*

Abstract. For low-level software code testing, a firmware model was developed for which unit testing and performance testing were performed. A comparison of the performance of the same software code on different hardware platforms was made. It has been suggested that developing and maintaining a firmware model for testing purposes may be more appropriate than testing directly on the device under development.
Keywords: *information security, software.*

Аналіз вимог є критичним для успішної розробки проекту. Вимоги мають бути задокументованими, вимірними, тестовними, пов'язаними з бізнес-потребами, і описаними з рівнем деталізації достатнім для конструювання системи. Функціональні вимоги – це перелік функцій або сервісів, які повинна надавати система, а також обмежень на дані і поводження системи при їхньому виконанні. Специфікація функціональних вимог – опис функцій та їхніх властивостей, які не містять у собі протиріч і виключень.

Для системи, що розробляється були сформульовані наступні функціональні вимоги:

1) засіб повинен працювати в середовищі Windows;

2) засіб повинен виконувати шифрування файлів та каталогів, при чому: користувач повинен мати змогу обрати носій, на якому будуть збережені дані; користувач повинен мати змогу обрати ключ шифрування;

3) засіб повинен виконувати дешифрування своїх криптоконтейнерів, при чому: засіб повинен працювати навіть якщо користувач не знає алгоритму шифрування та тип криптоконтейнера, але знає лише ключ шифрування; засіб повинен перевіряти ключ шифрування так, щоб у випадку помилкового ключа користувач отримував про це інформацію; засіб повинен мати змогу перевіряти цілісність криптоконтейнеру.

Архітектура програмного забезпечення містить такі важливі визначення [12]:

– організації системи програмного забезпечення;

– структурних елементів і їх інтерфейсів, з яких система складається, їх поведінка у взаємодії;

– склад цих елементів у великих підсистемах;

– архітектурний стиль, який визначає це ПЗ, його елементи і їх інтерфейси, їх взаємодія та їх склад.

Архітектура програмного забезпечення стосується не тільки структури та поведінки, а й використання, функціональності, продуктивності, стійкості, повторного використання, зрозумілості, економічних і технологічних обмежень, компромісів і естетики ПЗ. Системна архітектура – частина загальної архітектури ПЗ. Вона може бути представлена у виді кортежу, який задається наступною множиною:

$$SA = \langle C, F, I \rangle ,$$

де: С – множина програмних компонентів, які реалізовані на різних мовах програмування та виконують задану функціональність системи; F – множина допустимих структурних взаємодій, в яких можуть бути об'єднані елементи з множини С; I – множина зовнішніх інтерфейсів, які дана система надає зовнішнім системам, компонентам, користувачам.

Автори розглядав наступні патерни системних архітектур:

– standalone application. Всі дані зберігаються та обробляються в одному місці;

– 2-tier application. Обробка даних може проходити завдяки серверу;

– 3-tier application. Обробка та збереження даних забезпечується відповідними серверами.

Обрано трирівневу архітектуру завдяки наступним перевагам:

1) збереження даних відбувається на зімнному носії, який легко замінити в разі поломки, сховати або знищити; 2) шифрування даних відбувається на спеціальному сервері. Він захищений від втручань в свою роботу: мінімум комунікаційних інтерфейсів та програмного забезпечення; 3) «Тонкий» клієнт є менш вразливим, адже уся робота по збереженню і шифруванню відбувається в іншому місці.

Авторами розглядав дві альтернативні методології розробки ПЗ:

– RUP – Rational Unified Process;

– RAD – Rapid Application Development.

Для обміну між клієнтом та сервером потрібно використати готову реалізацію транспортного протоколу, або розробити власну. В ході виконання роботи було вирішено орієнтуватися на протокол UDP, бо він простий в реалізації та добре підходить в для цілей тестування і налагодження, бо не потребує підтвердження про доставку і має зрозумілу, мінімалістичну структуру.

Існує безліч апаратних засобів, за допомогою яких може бути реалізоване "прозоре" шифрування з записом на знімний носій. Серед умов розробки значиться реалізація на "слабкій" апаратній платформі, доступ до якої не обмежується ціною та часом входження в розробку, тому розглядалися не всі доступні засоби. Таким чином вибір пав на процесор ATmega 2560 на більш розповсюдженій налагоджувальній платі Arduino MEGA 2560. ATmega 2560 – це розповсюджений 8-бітний мікроконтролер з 256 kB flash пам'яті, 4 kB EEPROM енергонезалежної пам'яті та 8 kB SRAM ("оперативна" пам'ять). З такими характеристиками контролер потребує

лише 1.8 V 500 μ. А живлення, тож може працювати навіть від акумуляторних батарей. Жорсткі обмеження змушують використовувати не складні алгоритми та низькорівневі технології розробки.

Діаграма розгортання – діаграма, на якій представлені вузли системи. Діаграма розгортання застосовується для подання загальної структури і топології системи і містить зображення розміщення компонентів по окремих вузлах системи. Крім того, діаграма розгортання показує наявність фізичних з'єднань – маршрутів передачі інформації між апаратними засобами, задіяними в реалізації системи.

Діаграма класів (class diagram) служить для представлення статичної структури моделі системи в термінології класів об'єктно-орієнтованого програмування. На цій діаграмі показують класи, інтерфейси, об'єкти й кооперації, а також їхні відносини. Клієнтське ПЗ (”тонкий” клієнт) є об'єктно-орієнтованим, тож для нього побудована діаграма класів, яку наведено на рисунку 1.

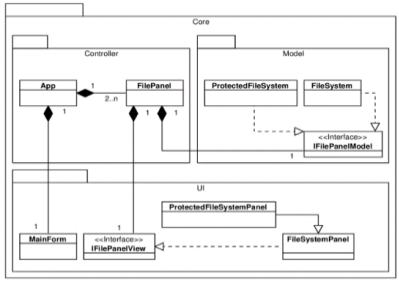


Рисунок 1 – Узагальнена діаграма класів клієнтського ПЗ

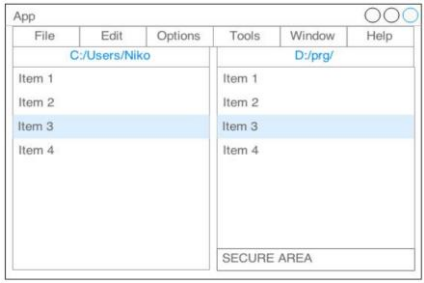


Рисунок 2– Mockup головного вікна інтерфейсу клієнтського ПЗ

«File System Panel» та «Protected File SystemPanel» з пакету ”UI” репрезентують інтерфейс користувача, а саме – панелі файлового менеджеру: загальну, для файлів користувача, та безпечну, для з'єднання та синхронізації з безпечним пристроєм. За отримання даних з відповідних файлових систем відповідають класи ”FileSystem” та ”Protected FileSystem” з пакету ”Model”. Клас ”App” за пакету ”Controller” містить контролер програми. Для кожної файлової панелі передбачено контролер ”File Panel”. Так як програмне забезпечення представляє собою двопанельний файловий менеджер (як показано на рисунку 2.), на діаграмі відображена уніфікація подібного роду панелей за допомогою інтерфейсу ”IFile PanelView”. Архітектура додатку в цілому відповідає патерну MVC.

Мікропрограмне забезпечення повинно бути максимально низькорівневим, тому його зазвичай розробляють за допомогою таких мов програмування як Assembler, C та C++. Автори роботи вирішили, що для скорочення часу на розробку прототипу доцільно буде використовувати найбільш простий інструмент – мову C++. Для спрощення роботи з конкрет-

ною апаратною платформою автор використовував Arduino SDK. Мікропрограмне забезпечення не є об'єктно-орієнтованим через те, що апаратні ресурси платформи, на якій програма буде виконуватись, можуть бути сильно обмежені. З тією ж ціллю внутрішній протокол обміну з комп'ютером розроблено без збереження стану між передачами.

Програмне забезпечення використовує особливості розробленого протоколу: перевіряє цільову адресу пакету, контрольну суму, порт. Для реалізації комунікації за розробленим протоколом була розроблена бібліотека «libNetwork». Вона виконує перевірки контрольних сум та визначає обробник, до якого будуть передані дані. Згідно діаграми, мікропрограмне забезпечення постійно працює в режимі очікування команди з мережі. Після одержання даних виконується виділення необхідного об'єму пам'яті (якщо є така кількість вільної пам'яті), перевірка контрольної суми, передача пакету до належного обробника. Останній, якщо це необхідно, може сформувати власний пакет і надіслати його у відповідь.

Для тестування низькорівневого програмного коду розроблена модель мікропрограмного забезпечення, для якої проводиться модульне тестування, та тестування швидкодії. Проведене порівняння швидкодії однакового програмного коду на різних апаратних платформах. Висунуто припущення, що розробка та підтримка моделі мікропрограмного забезпечення в цілях тестування може бути більш доцільною, ніж тестування безпосередньо на пристрої, що розробляється.

Література

1. Zachko I., Ivanusa A., Zachko O. Models and mechanisms management of program projects of socio-economic development the territories // Scientific Journal of Astana IT University. – Astana, 2020. – V. 3. – pp. 110-116.

2. Kobylkin, D., Zachko, O., Ratushny, R., Ivanusa, A., Wolff, C. Models of content management of infrastructure projects mono-templates under the influence of project changes // CEUR Workshop Proceedingsthis link is disabled, 2021, V. 2851, pp. 106–115.

3. Інформаційні технології в управлінні проєктами безпечної експлуатації об'єктів масового перебування людей. – Монографія. – Львів : Вид-во ЛДУ БЖД, 2023. – 306 с.

4. Івануса А. І., Яковчук Р. С., Ємельяненко С. О., Івануса З. З. Управлінські та інформаційні особливості проекту безпечної експлуатації спортивно-видовищних споруд. Науковий вісник НЛТУ України. 2019, т. 29, № 8. С. 134–141.

5. Ivanusa, A., Marych, V., Kobylkin, D., & Yemelyanenko, S. (2023). Construction of a visual model of people's movement to manage safety when evacuating from a sports infrastructure facility. Eastern-European Journal of Enterprise Technologies, 2(3 (122), 28–41. https://doi.org/10.15587/1729-4061.2023.277492.

6. Ivanusa A. «Project of forming «culture and safety» of the airport» // MATEC Web of Conferences, V. 247, 00045 (2018) https://doi.org/10.1051/matecconf/20182470004.

УДК 004.056.5:005

ДОСЛІДЖЕННЯ ПРОЦЕСУ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Івануса Андрій, Ящук Валентина, Федина Богдана
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи оцінювання ризиків кібербезпеки об'єктів критичної інфраструктури. Визначено сучасні підходи до оцінювання ризиків кібербезпеки об'єктів критичної інфраструктури. Наведено методичні підходи до формування концепції оцінювання ризиків кібербезпеки об'єктів критичної інфраструктури. Запропоновано етапи вирішення науково-практичної проблеми, пов'язаної з підвищенням рівня захисту інформаційних систем критичної інфраструктури шляхом розроблення методології забезпечення кібербезпеки об'єктів критичної інфраструктури.

Ключові слова: захист інформації, кібербезпека, оцінювання ризиків, комплексний ризик, об'єктивний ризик, суб'єктивний ризик, інформаційна система, управління ризиком.

The theoretical, scientific-methodical, and organizational-functional bases of cyber security risk assessment of critical infrastructure objects are considered. Modern approaches to cyber security risk assessment of critical infrastructure facilities are defined. Methodical approaches to the formation of the concept of cyber security risk assessment of critical infrastructure objects are given. The stages of solving the scientific and practical problem associated with increasing the level of protection of information systems of critical infrastructure by developing a methodology for ensuring cyber security of critical infrastructure objects are proposed.

Keywords: information protection, cyber security, risk assessment, complex risk, objective risk, subjective risk, information system, risk management.

Події останніх років в Україні і у світі показали нагальну необхідність забезпечення безпеки об'єктів критичної інфраструктури, особливо енергетичного сектору. Сьогодні, коли ворог завдає ракетних ударів по об'єктам критичної інфраструктури та атакує інформаційні системи об'єктів китичної інфраструктури, питання забезпечення безпеки об'єктів критичної інфраструктури шляхом оцінювання ризиків є актуальним.

Законодавство України про критичну інфраструктуру (КІ) спрямоване на впорядкування питань, пов'язаних з об'єктами КІ. Однак більшість норм та механізмів, передбачених цим законодавством, станом на сьогоднішній день не працюють. Основною причиною цього є збройна агресія російської федерації проти України. В умовах війни уряд має більш пріо-

ритетні задачі, ніж забезпечення функціонування законодавства про КІ. Закон про КІ набув чинності в червні 2022 року, але не пройшов практичного застосування. Уповноважений орган у сфері захисту КІ, який повинен був бути створений у березні 2022 року, був створений лише в липні 2022 року, але не функціонує. Також не затверджені окремі порядки, які стосуються Реєстру та паспортизації об'єктів КІ.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» забезпечення кібербезпеки об’єкту критичної інфраструктури, у тому числі енергетичного сектору, досягається створенням системи управління інформаційною безпекою (СУІБ) у відповідності до міжнародного стандарту ISO/IEC 27001:2013 або створенням комплексної системи захисту інформації (КСЗІ) у відповідності до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах». Одним з основних етапів побудови СУІБ, КСЗІ є створення системи управління ризиками.

Оцінювання ризиків кібербезпеки інформаційних систем, у тому числі об’єктів критичної інфраструктури, є складною проблемою, яка актуальна для всього світу. Існуючі методи оцінювання не завжди дають точні результати, оскільки не враховують усі фактори, які можуть впливати на кібербезпеку. Однією з основних проблем є те, що існуючі методи не дозволяють оцінити суму ризиків. Це ускладнює кількісне оцінювання ризику проекту або процесу. Крім того, існуючі методи не враховують вплив людського чинника, який може призвести до кібератаки. Оцінювання ризику кібербезпеки зазвичай здійснюється на підставі статистичних даних кіберінцидентів. Однак такі дані не завжди доступні, особливо для критичної інфраструктури. Крім того, навіть якщо такі дані є, вони можуть не відображати реальну величину збитків від кібератаки.

Вирішення науково-практичної проблеми, пов’язаної з підвищенням рівня захисту інформаційних систем критичної інфраструктури шляхом розроблення методології забезпечення кібербезпеки інформаційних систем об’єктів критичної інфраструктури ми пропонуємо здійснювати за такими етапами:

- проаналізувати сучасні методи, методики, методології оцінювання ризиків кібербезпеки інформаційних систем, у тому числі об’єктів критичної інфраструктури, а також програмні продукти управлінням такими ризиками.
- обґрунтувати поняття комплексного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури, здійснити його змістовну інтерпретацію та розглянути основні властивості.
- розробити методи обчислення сумарного ризику кібербезпеки інформаційних систем об’єктів критичної інфраструктури з використанням значення максимальних наслідків.

- розробити методологію оцінювання ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням розроблених методів.
- розробити структурні рішення обчислювальних систем для розрахунку сумарного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням розроблених методів.
- розробити алгоритмічне та програмне забезпечення обчислювальних систем для розрахунку сумарного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури з використанням розроблених методів.
- провести експериментальні дослідження з метою підтвердження теоретичних положень та практичних розробок дослідження.

Сучасні підходи до оцінювання ризиків кібербезпеки об'єктів критичної інфраструктури спрямовані на врахування всіх факторів, які можуть впливати на кібербезпеку, включаючи людський чинник; оцінювання суми ризиків, що дозволяє здійснювати кількісне оцінювання ризику проекту або процесу; застосування даних про реальні кіберінциденти, що дозволяє отримати більш точні оцінки ризиків; використання автоматизованих інструментів, що дозволяє підвищити ефективність і швидкість оцінювання ризиків; інтеграцію оцінювання ризиків з іншими процесами управління кібербезпекою. Ці підходи дозволяють власникам об'єктів критичної інфраструктури краще розуміти ризики, яким вони піддаються та розробляти ефективні заходи захисту. Реалізація запропонованих заходів підвищить ефективність оцінювання ризиків кібербезпеки об'єктів критичної інфраструктури.

Література

1. Закон України «Про критичну інфраструктуру» (1882-IX від 16.11.2021), який набрав чинності 15.12.2021, але почав діяти тільки 15.06.2022 [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1882-20#n20

2. Постанова КМУ від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури», зі змінами від 29.12.2021, яка набула чинності 31.12.2021 [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

3. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю.Драб, В. Ящук // 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 621.396.4

ВИКОРИСТАННЯ АЛГОРИТМІВ ШІ ДЛЯ АНАЛІЗУ ШКІДЛИВОГО ТРАФІКУ НА КАНАЛЬНОМУ РІВНІ (ARP SPOOFING)

Івченко Олександр, Палагін Володимир
Черкаський державний технологічний університет

Розглянуто рішення, яке базується на використанні штучного інтелекту (ШІ) для класифікації та виявлення зловмисного мережевого трафіка, згенерованого в результаті атаки ARP spoofing. Наведено типові загрози комп'ютерним мережам фізичного та канального рівнів моделі OSI та проведено аналіз особливостей виявлення таких загроз з використанням методів ШІ. Результати аналізу можуть бути використані для прийняття обґрунтованих рішень щодо вибору методів захисту для мереж різного призначення та з різними вимогами щодо захисту інформації.

Ключові слова: Аналіз трафіку, ARP spoofing, штучний інтелект, атаки на рівні L2, MAC-адреса

A solution based on the use of artificial intelligence (AI) for the classification and detection of malicious network traffic is considered. ARP spoofing is considered malicious network traffic. Typical threats to computer networks at the physical and channel levels of the OSI model are given, and the features of detecting such threats using AI methods are analyzed. The results of the analysis can be used to make informed decisions about the choice of protection methods for networks of different purposes and with different requirements for information protection.

Keywords: Traffic analysis, ARP spoofing, artificial intelligence, L2 level attacks, MAC address

Пристрої мережі, які працюють на другому рівні еталонної моделі OSI вважаються найслабшою ланкою в інфраструктурі безпеки [1-3, 6]. Розповсюджена IT-політика BYOD, використання віртуальних мереж і низки складних атак, збільшують вірогідність того, що мережі стають більш уразливими до проникнення саме на рівні L2. Протоколи рівня L2 дуже часто залишаються без належної уваги і здебільшого працюють зі стандартною конфігурацією. Слід пам'ятати, що порушення мережної безпеки на рівні L2 також впливатиме на всі рівні, розташовані вище. Таким чином, фахівцям з мережної безпеки потрібно також запобігати і вчасно нейтралізувати атаки на інфраструктуру LAN рівня L2.

В роботі наведена можливість аналізу основних загроз безпеці пристроїв рівня 2 з використанням засобів штучного інтелекту (*ШІ*). Використання такого підходу полягає в аналізі трафіку, який проходить через мережеві пристрої рівня L2. Аналіз трафіку і прийняття рішення про його шкідливість здійснюється засобами *ШІ*. Модель, яку буде вивчати *ШІ*, можна задати у відповідності до можливих мережевих атак на рівні L2.

Атака *ARP spoofing*, також відома як «*отруєння кешу*» *ARP*, використовується в атаці типу «людина посередині» [5, 6]. Під час атаки *ARP spoofing* зловмисник діє наступним чином: надсилає небажане, підроблене повідомлення відповіді *ARP*, яке містить підроблену MAC адресу машини зловмисника для всіх хостів у локальній мережі. Після отримання відповіді *ARP* усі пристрої в локальній мережі оновлять свої *ARP* або таблиці MAC-адрес із неправильною MAC-адресою. Це ефективно *«отруює кеш»* на кінцевих пристроях. Якщо таблиці *ARP* «*отруєні*», це дозволить зловмиснику видати себе за інший хост, щоб отримати доступ до конфіденційної інформації.

На наведеному нижче рисунку (рис.1) представлена атака ARP. Зловмисник надіслав фальшиву відповідь, яка «*отруїла кеш*» в пристроях. Усі хости в мережі тепер думають, що 10.40.10.103 знаходиться на 46:89:FF:4C:57, замість 00:80:68:B4:87.

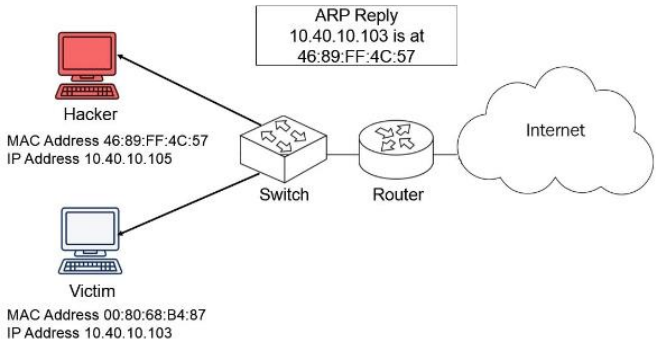


Рисунок 1 – Атака *ARP spoofing*

Щойно зловмисник почне отримувати трафік, спрямований на інший хост, він використовуватиме засоби, щоб зібрати неправильно спрямований трафік у спробі отримати конфіденційну інформацію.

Виявлення трафіку, який спричинений атакою *ARP spoofing*, є досить складною операцією, так як потребує аналізу і виявлення шкідливого трафіку при активізації атаки *ARP spoofing* (початковий етап «*отруєння ARP кешу*»), аналізу і виявлення самого факту, що трафік переадресовується через вузол зловмисника. Щоб виявити цю загрозу використовують системи виявлення вторгнень, які спеціально налаштовані на вирішення подібного завдання. Альтернативою таких систем є застосування програмного забезпечення, що працює на пристроях, яке призначене для виявлення раптових змін в елементах ARP-таблиці [5,6].

Пропонуються спеціалізовані програмні рішення, які базуються на застосуванні моделей машинного навчання, які своєчасно класифікують і

виділяють подібні атаки та створюють керуючі сигнали для їх запобігання. Розробка та застосування таких моделей *ШІ дозволяє автоматизувати аналіз* мережевого трафіка та підвищити безпеку комп'ютерних мереж.

Висновки. Розглянута можливість використання засобів *ШІ* для виявлення мережевого трафіку, спричиненою атакою *ARP spoofing*. Така атака може спричинити перебої в роботі мережі і сприяти перехопленню інформації зловмисниками, яким вдалося проникнути в область дії рівня L2. Таким чином, розробка і застосування ефективних моделей машинного навчання для виявлення і попередження подібних атак є перспективним і надійним інструментом для захисту мережних пристроїв канального рівня і моніторингу роботи мережі.

Література

1. Wendell Odom. CCNA 200-301 Official Cert Guide. Volume 1-2 Cisco Press, 2019. — 1095 p.

2. Chris Carthern, William Wilson, Richard Bedwell, Noel Rivera Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA. Apress Media, 2015. — 839 p.

3. Omar Santos, John Stuppi CCNA Security 210-260 Official Cert Guide. Apress Media, 2016. — 608 p.

4. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013. — 256 с.

5. Chris Sanders, Practical packet analysis. Using wireshark to solve real-world network problems. 3-d Edition, 2019. — 448 pages

6. Lisa Bock, Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark, 2nd Edition, 2022. — 606 pages

УДК 331.108

ТРУДОВІ РЕСУРСИ ПІДПРИЄМСТВА: СТРУКТУРА, СУТНІСТЬ ТА ЇХ ВПЛИВ НА ДІЯЛЬНІСТЬ ПІДПРИЄМСТВА

Карабін Богдан
Академія праці, соціальних відносин і туризму (Київ, Україна)

Анотація. *Розглянуто структуру, сутність і класифікацію трудових ресурсів підприємства. Описано кількісні та якісні характеристики трудових ресурсів підприємства. Визначено роль трудових ресурсів у підвищенні прибутковості та конкурентоздатності підприємства.*

Ключові слова: *підприємство, ефективність, трудові ресурси, фаза, кількісні та атрибутивні характеристики.*

Annotation. The article is devoted to the issues of using labor resources in the enterprises. *Described the structure, essence and classification of labor resourcesin in an enterprise. Given the quantitative and qualitative characteristics of labor resources in an enterprise. Presented the role of labor resources in increasing the profitability and competitiveness of an enterprise*

Keywords: *enterprise, efficiency, labor resources, phase, quantitative and attributive properties.*

Найбільш важливим елементом розвитку економіки і головним джерелом продуктивних сил є люди, їх освіта, майстерність, мотивація діяльності, підготовка. Існує непересічна залежність конкурентоспроможності економіки, рівня добробуту населення від якості трудового потенціалу персоналу підприємства, організації.

Людські ресурси підприємства є головним ресурсом будь-якого підприємства, від якості та ефективності якого, зазвичай, залежать результати діяльності підприємства. Людський фактор – в оптимальному поєднанні з природним і матеріально-технічним – є тією вихідною ланкою, яка створює основну рушійну міць становлення, розвитку і ефективного господарювання всіх соціально-економічних укладів у сільській місцевості. Водночас розвиток різноукладності в умовах ринку становить підвищені вимоги до якостей людини як носія і персоніфікованого власника робочої сили, що використовується у процесі створення споживних вартостей у формі товарів або послуг.

Певний внесок у розробку означеної проблеми зробили вчені Є. Балацький, В. Авдєєнко, С. Писаренко, С. Бандура, В. Котлова, О. Шаблій, Ф. Заставний, М. Пітюлич. Їх бачення та висвітлення проблем є нетрадиційним, оригінальним і новаторським.

Метою тез є визначення сутності трудових ресурсів підприємства та їх впливу на діяльність підприємства.

Інформаційні технології є частиною сучасного життя не тільки людини, а й бізнес-процесів. Використання інформаційних технологій в управлінні підприємством здійснюється з метою ефективної та оперативної комп'ютерної обробки інформаційних ресурсів, зберігання великих

обсягів економічно важливої інформації та передачі її на будь-які відстані в мінімальні терміни. Тобто основним завданням є оптимізація діяльності підприємства на основі застосування інформаційних технологій [6; 7; 8]. До основних переваг використання інформаційних технологій в управлінні підприємством можна віднести:

1) підвищується керованість;

2) знижується вплив людського фактора;

3) скорочується паперова робота;

4) підвищується оперативність і достовірність інформації, важливої для прийняття ключових рішень;

5) знижуються витрати.

Найбільш важливим елементом продуктивних сил і головним джерелом розвитку економіки є люди, їх майстерність, освіта, підготовка, мотивація діяльності. Трудові ресурси – це частина працездатного населення, що за своїми віковими, фізичними, освітніми даними відповідає тій чи іншій сфері діяльності.

Структура трудових ресурсів може розглядатися за різними ознаками: віку, статі, освіти, професії, релігії, зайнятості за сферами економіки, місцю проживання тощо [4]. Структура трудових ресурсів з економічної погляду відображено на рис. 1.

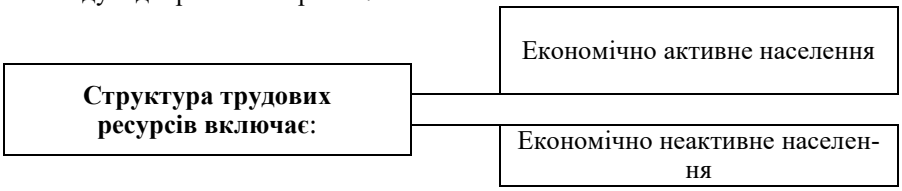


Рисунок 1 – Структура трудових ресурсів.
Укладено автором особисто

Економічно активне населення – це сукупність працездатних зайнятих і безробітних громадян, що забезпечують пропозицію робочої сили на ринку праці для товарного виробництва і сфери послуг у певному періоді.

Економічно неактивне населення - це населення, що за будь-яких причин не створює пропозиції робочої сили на ринку праці. Звичайно, до економічно неактивного населення відносять такі його категорії:

1) пенсіонери за віком та інших категорій, відповідно до національного трудового законодавства;

2) учні і студенти денної форми навчання;

3) працівники домашніх господарств і працюючі по догляду за дітьми, хворими тощо;

4) інваліди відповідних груп (відповідно до законодавства);

5) непрацюючі особи, що за будь-яких причин припинили пошук роботи (вичерпали всі можливості знайти підходящу роботу, лишили надію знайти роботу);

6) забезпечені особи? в котрих немає необхідності (бажання) працювати з метою одержання трудового доходу [3].

Розрізняють такі фази відтворення трудових ресурсів: фаза формування, фаза розподілу і перерозподілу і фаза використання.

Фаза формування характеризується природним і механічним відтворенням трудових ресурсів, відновленням спроможності до праці реальних працівників і одержанням людьми освіти, фаху і трудової кваліфікації.

Фаза розподілу і перерозподілу в умовах ринкової економіки, в основному, забезпечується функціонуванням ринку праці і характеризується розподілом робочої сили по сферах зайнятості, галузям економіки, видам робіт, підприємствам, регіонам і районам країни.

Фаза використання полягає у використанні економічно активного населення на конкретних підприємствах і в економіці в цілому.

Існують екстенсивний та інтенсивний типи відтворення трудових ресурсів.

Екстенсивний тип відтворення характеризується збільшенням чисельності трудових ресурсів без зміни їхніх якісних характеристик.

Інтенсивний тип відтворення передбачає зміну якісних характеристик робочої сили. До них відносять: ріст освітнього рівня робітників, їхньої кваліфікації, фізичних і розумових спроможностей та ін. [1]. Персонал підприємства є найбільш цінним ресурсом підприємства, через що вимагає особливого підходу у питаннях управління. Кадри (персонал) підприємства – це сукупність постійних працівників. що отримали необхідну професійну підготовку та (або) мають досвід практичної діяльності. Класифікацію персоналу (кадрів) підприємства відображено на таблиці 1.

Таблиця 1

Класифікація персоналу підприємства

Ознака	Види
За характером участі в господарській діяльності	Виробничий персонал - включає працівників основних, допоміжних та обслуговуючих виробництв, заводоуправління, складів, охорони – тобто всіх зайнятих у виробництві або його безпосередньому обслуговуванні.
	Невиробничий персонал – Включає працівників структур, які хоч і перебувають на балансі підприємства, але не пов'язані безпосередньо з процесами промислового виробництва: житлово- комунальне господарство, дитячі садки та ясла, амбулаторії, навчальні заклади тощо.
По відношенню до виробництва	Основні робітники – безпосередньо беруть участь у процесі створення продукції.
	Допоміжні робітники – виконують функції обслуговування основного виробництва

За статтю	Чоловіки
	Жінки
За характером виконуваних функцій	Керівники
	Спеціалісти
	Службовці
	Робітники

Укладено автором за джерелом [2]

Показники, що характеризують склад, обсяг та рух персоналу у часі зображено на Рис. 2

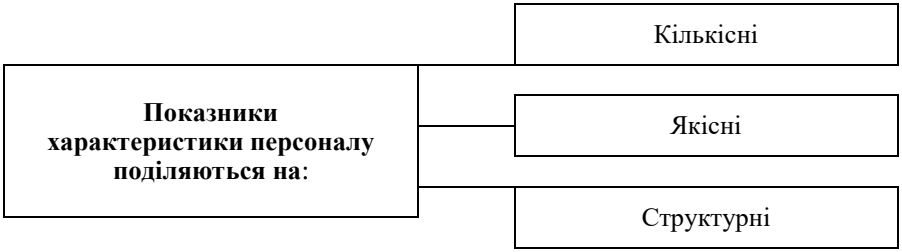


Рисунок 2 – Показники, які характеризують персонал підприємства
Розроблено автором за джерелом [5]

До кількісних показників характеристики чисельності персоналу підприємства відноситься:

1) *явочна чисельність працівників* (включає всіх працівників, що з'явилися на роботу).

2) *облікова чисельність працівників*: включає всіх постійних, тимчасових і сезонних працівників, котрих прийнято на роботу терміном на один і більше днів незалежно від того, перебувають вони на роботі, знаходяться у відпустках, відрядженнях, на лікарняному листку тощо.

3) *середньооблікова чисельність працівників,* що визначається як сума середньомісячної чисельності за певний період, поділена на кількість місяців у періоді.

Висновки. Отже, трудові ресурси характеризуються сукупністю специфічних властивостей, насамперед, пов’язаних з їхнім економіко-соціальним характером, який головним чином виявляється у відмінностях трудових від решти економічних ресурсів. Інвестування у розвиток людського капіталу дає можливість досягти не тільки короткострокового економічного успіху, а й закласти основу для формування позитивних довгострокових тенденцій у розвиток національної економіки і кожного підприємства зокрема. Тому, необхідно розробляти стратегії управління персоналом з урахуванням сучасного світового досвіду, створювати нові системи навчання і розвитку персоналу підприємства. Вкладення коштів у розвиток

трудових ресурсів підвищить рівень ефективності підприємств як на внутрішньому, так і на зовнішніх ринках. Державна політика має бути спрямована на стимулювання підприємств.

Література

1 Аналіз ефективності використання трудових ресурсів у системі управління діяльністю автотранспортних підприємств. *Наукові записки: зб. наук, праць кафедри економічного аналізу Тернопільського національного економічного ун-ту*. 2019. Вип. 16. С. 293–294.

2. Гетьман О. О., Шаповал В. М. Економіка підприємства [Текст] : навчальний посібник. Київ: Центр учбової літератури, 2018. 488 с.

3. Гринькова В. М., Ястремська О. М. Проблеми управління трудовими ресурсами підприємства: наук. вид. Харків: ХНЕУ, 2016. 192 с.

4. Давидюк Т. В. Трудові ресурси, трудовий потенціал, робоча сила, людський капітал: взаємозв'язок категорій. *Вісник Житомирського державного технологічного університету*. 2020. № 1(47). С. 30–35.

5. Іванілов О. С. Економіка підприємства: підруч. [для студ. вищ. навч. закл.]. Київ: Центр учбової літератури, 2018. 728 с.

6. Петько С. М. Роль центрів інформаційної безпеки в захисті ІТ-інфраструктури компаній. Інформаційна безпека та інформаційні технології: матеріали IV Міжнародної наук.-практ. конференції (м. Львів, 30 листопада 2022) /Львівський державний університет безпеки життєдіяльності. Львів: Растр-7, 2022. С. 81–83.
URI: https://ir.kneu.edu.ua:443/handle/2010/39266

7. Петько С М. Теоретичні основи цифрової трансформації суб'єктів господарювання. Економіка та суспільство.2023. № 47. DOI: https://doi.org/10.32782/2524-0072/2023-47-55

8. Петько С. М. «SMART-factories» у післявоєнному відновленні України [Електронний ресурс]. *Інформаційні технології: теорія і практика* : тези доп. VI Всеукр. Інтернет-конф. здобувачів вищ. освіти і молод. учених (м. Харків, 23–24 берез. 2023 р.) / М-во освіти і науки України, Харків. нац. ун-т міськ. госп. ім. О. М. Бекетова [та ін.] ; [редкол.: М. В. Новожилова та ін.]. Електрон. текст. дані. Харків : ХНУМГ ім. О. М. Бекетова, 2023. С. 21–24. – Назва з титул. екрана. URI: https://ir.kneu.edu.ua:443/handle/2010/40097

УДК: 004.056.55

ФІШИНГ ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ АТАК В КІБЕРПРОСТОРІ

Кирилюк Артем, Онацький Олексій
Державний університет інтелектуальних технологій і зв'язку, м. Одеса

Анотація. Дослідження сучасних методів кібератак, зокрема фішингу, виявляє актуальність та загрози для інформаційної безпеки, а також роль соціального інженерінгу та зростання глобальної уваги до кібербезпеки. У роботі висвітлює необхідність ефективних захисних засобів, вивчення психологічних аспектів та спільних зусиль для забезпечення інформаційної безпеки.

Ключові слова: кіберпростір, захист, фішинг, загроза, фішингова атака, соціальна інженерія, глибоке навчання.

Key words: cyberspace, protection, phishing, threat, phishing attack, social engineering, deep learning.

У сучасному світі, роль кіберпростору надзвичайно важлива, і разом з нею зростає імовірність кібератак. Інтернет та комп'ютерні технології стали неодмінною складовою життя, але разом із ними з'явилися загрози, пов'язані зі зловживанням цими технологіями. Однією з найпоширеніших і найбільш актуальних методів атак в кіберпросторі є фішинг [1]. Ця методика на сьогоднішній день є серйозною загрозою для інформаційної безпеки і приватності користувачів. Фішингові атаки стають все більш вдосконаленими та субтельними, тому дослідження сучасних методів атак в кіберпросторі, зокрема фішингу, має велике значення для забезпечення безпеки та захисту інтернет-користувачів. У цьому дослідженні ми докладніше розглянемо сутність та небезпеки фішингу, вивчимо його сучасні методи та засоби захисту від цієї загрози.

За останні роки спостерігається стійке зростання кількості фішингових атак, і це свідчить про постійну актуальність цієї проблеми [2]. Зловмисники адаптуються до нових технологій та розвивають більш хитрі способи введення користувачів в оману.

Фішингові атаки нерідко використовують соціальний інженеринг для психологічного впливу на потенційну жертву. Соціальна інженерія може бути реалізована багатьма способами, у тому числі через Інтернет, по телефону, особисто або за допомогою традиційної пошти. Поширена мета соціальної інженерії – перехоплення облікових даних користувача у процесі фішингу. Цей підхід стає все більш важливим для розуміння фішингу, оскільки зловмисники намагаються використовувати емоційний та психологічний вплив для досягнення своїх цілей.

Розвиток засобів захисту від фішингу [2, 3] стає необхідним завдяки

поширенню цієї загрози. Антивіруси, антиспам-фільтри, навчальні програми для користувачів та технології аналізу трафіку постійно вдосконалюються для виявлення та запобігання фішинговим атакам.

Також потрібно розуміти, що любі кібер-атаки можуть мати серйозні глобальні наслідки, включаючи крадіжку конфіденційної інформації, фінансові втрати та порушення приватності. Тому вивчення цієї проблеми стає національним і міжнародним пріоритетом у галузі кібербезпеки.

Дослідження сучасних методів атак в кіберпросторі, зокрема фішингу, можуть включати такі аспекти:

1) Аналіз сучасних фішингових методів. Дослідження конкретних методів, таких як spear-phishing, vishing, або SMS-фішинг [4, 5], для розуміння їхньої ефективності та поширеності.

2) Вивчення психологічних аспектів фішингу. Дослідження впливу соціального інженерингу на користувачів та розробка психологічних стратегій захисту.

3) Оцінка ефективності засобів захисту. Аналіз різних засобів захисту від фішингу, включаючи: традиційні методи (наприклад, чорні та білі списки); антивіруси; антиспам-фільтри; методи машинного та глибокого навчання (deep learning) [6] та розробка рекомендацій для їх оптимального використання.

4) Створення навчальних програм. Навчання протистояння фішингу – один із найкращих, найважливіших засобів захисту. Розробка освітніх матеріалів та навчальних програм для підвищення освіченості користувачів щодо фішингових загроз та засобів їх запобігання. Навчання може включати такі теми, як: розпізнавання підроблених електронних листів, ідентифікація фішингових веб-сайтів та методів обману користувачів. Важливо навчати користувачів основ захисту даних, щоб вони могли краще розпізнати атаки фішинга.

5) Аналіз глобальних трендів та використання інтелігентних аналітичних інструментів для виявлення нових загроз. Спостереження за розвитком фішингових атак у різних країнах та розробка систем виявлення нових атак.

6) Публікація результатів та спільна співпраця. Ділитися результатами досліджень та співпрацювати з іншими дослідниками, урядовими органами та компаніями для обміну даними та розробки спільних стратегій боротьби з фішингом.

Моя особиста думка щодо дослідження сучасних методів атак в кіберпросторі, зокрема фішингу, полягає в тому, що ця проблема стає все більш актуальною та складною. З розвитком технологій зловмисники постійно вдосконалюють свої методи та стають більш витонченими у веденні атак. Особисто мене турбує збільшення кількості соціального інженерингу в фішингових атаках, оскільки цей метод може викликати велику довіру у потенційних жертв, зробивши їх менш обачними.

Фішинг є актуальною проблемою, оскільки шкідливі програми та методи соціальної інженерії [7], що використовуються при цих атаках, можуть завдати значної шкоди. Також важливо відзначити, що фішингові атаки можуть бути спрямовані на широкий спектр цілей, від індивідуальних користувачів до великих корпорацій та державних структур. Це створює ризик для приватності та безпеки всього суспільства. Тому, на мою думку, забезпечення ефективного захисту від фішингових атак має стати пріоритетом для багатьох сфер, включаючи урядові органи, бізнес та індивідуальних користувачів.

Залучення більше уваги до освіти щодо кібербезпеки також вважаю дуже важливим. Інформування користувачів про ризики та навчання їх розпізнавати фішингові спроби може суттєво зменшити успішність цих атак. Таким чином, об'єднані зусилля на рівні освіти, технологій та політики можуть допомогти боротися з фішинговими атаками та підвищити загальний рівень кібербезпеки.

Література

1. Фішинг. URL: https://uk.wikipedia.org/wiki/Фішинг

2. Акерлоф Д., Шиллер Р. Фішинг. Хто і як маніпулює вашим вибором : Вид-во Наш Формат, 2017. 272 с.

3. Hadnagy C., Fincher M. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails : Published by John Wiley & Sons, 2015. 192 p.

4. Journal of Computer Security. URL: https://www.iospress.com/ catalog/journals/journal-of-computer-security

5. Computers & Security. URL: https://www.sciencedirect.com/ journal/computers-and-security

6. IEEE Security & Privacy. URL: https://ieeexplore.ieee.org/ xpl/RecentIssue.jsp?punumber=8013

7. Hadnagy C. Social Engineering: The Art of Human Hacking : Published by John Wiley & Sons, 2010. 298 p.

УДК 004.056

ОЦІНКА ЕФЕКТИВНОСТІ SOC ТА РЕКОМЕНДАЦІЇ ПО ЇЇ ПІДВИЩЕННЮ

Козачок Юлія
Сумський державний університет

Мета роботи – оцінка ефективності SOC та розробка рекомендацій щодо її підвищення.
Результати роботи: було проведено інформаційний огляд основних принципів функціонування SOC, визначено критерії оцінки ефективності, проведено її вимірювання (а саме: збір даних про діяльність SOC, аналіз цих даних, оцінка ефективності SOC за розробленими показниками) та надано рекомендації по її підвищенню.
Ключові слова: security operations center, кіберзагрози, корпоративна кібербезпека

В наш час, в умовах стрімкого розвитку інформаційних технологій, зростання кількості кіберзагроз та ускладнення їх характеру, зростає і роль центрів забезпечення та управління інформаційною безпекою (SOC). SOC – це команда, що складається в основному з аналітиків з безпеки, в завдання якої входить виявлення та аналіз інцидентів кібербезпеки, оперативне реагування, запобігання їх виникненню і складання звітності [1].

Ефективність SOC є ключовим чинником забезпечення кібербезпеки організації. Вона визначається сукупністю показників, що характеризують здатність своєчасно виявляти та реагувати на інциденти інформаційної безпеки. Основними критеріями ефективності SOC є: своєчасність виявлення кіберзагроз (SOC повинен бути здатний своєчасно виявляти кіберзагрози, щоб запобігти їхньому впливу на інформаційні системи та інфраструктуру), точність виявлення кіберзагроз, швидкість та ефективність реагування на них.

Рекомендації щодо підвищення ефективності SOC включають:

- Підвищення кваліфікації персоналу SOC (аналітики повинні мати високу кваліфікацію та бути в курсі останніх тенденцій у сфері кібербезпеки, а також постійно проходити навчання, щоб підвищувати рівень своєї компетенції);
- Впровадження сучасних технологій та інструментів;
- Автоматизацію процесів (потрібно автоматизувати все, що піддається автоматизації, адже це буде економити час аналітиків, який вони краще витратять на речі, що вимагають ручної та вдумливої роботи).

Неефективність SOC може призвести до негативних наслідків, таких як недооцінка загроз інформаційної безпеки (що знизить рівень захищеності організації) та втрата репутації. З урахуванням сутності проблеми та її негативних наслідків можна зробити висновок, що підвищення ефективності SOC є актуальним завданням для будь-якої організації, яка здійснює свою діяльність в умовах кіберзагроз.

Таким чином, оцінка ефективності SOC дозволяє виявити сильні та слабкі сторони системи, визначити напрями її подальшого розвитку та вдосконалення. Результати оцінки можуть бути використані для ухвалення управлінських рішень, спрямованих на підвищення ефективності SOC.

Література

1. SOC: що це таке і навіщо воно потрібне? *InDevLAB*. URL: https://indevlab.com/uk/blog-ua/soc-scho-tse-take-i-navischo-vono-potribne/ (дата звернення: 20.11.2023).

УДК 004.056.5

СУЧАСНІ ТЕНДЕНЦІЇ В РОЗВИТКУ КРИПТОГРАФІЧНИХ ТА СТЕНОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Копитко Данило, Головатий Роман
Львівський державний університет безпеки життєдіяльності, м. Львів

Досліджено важливість та актуальність захисту інформації в сучасному комп'ютерному середовищі, де криптоатаки стають загрозою через різноманітні методи, використовані зловмисниками - від соціальної інженерії до помилок у програмуванні. Описано різні методи криптографічного захисту даних, такі як симетричне та асиметричне шифрування, хешування, цифрові підписи та протоколи обміну ключами. Розроблено концепцію комплексного підходу до захисту інформації, підкреслено важливість постійного вдосконалення криптографічних стандартів для забезпечення безпеки в цифровому середовищі.

Ключові слова: криптоатаки, захист інформації, симетричне шифрування, асиметричне шифрування, хешування

Researched the importance and relevance of information protection in today's computer environment, where crypto attacks pose a threat through various methods used by perpetrators - from social engineering to programming errors. Described various methods of cryptographic data protection, such as symmetric and asymmetric encryption, hashing, digital signatures, and key exchange protocols. Developed a concept of a comprehensive approach to information protection, emphasizing the importance of continually improving cryptographic standards to ensure security in the digital environment.

***Keywords*:** crypto attacks, information security, symmetric encryption, asymmetric encryption, hashing

Для сучасного комп’ютерного співтовариства криптоатаки стали повсякденністю. Зловмисниками використовуються як методи соціальної інженерії для отримання необхідної інформації, так і помилки в адмінсіструванні та програмуванні. Всі засоби масової інформації останнім часом наповнено повідомленнями про атаки на інформацію, про хакерів і комп'ютерні взломи. Дати визначення цього явища дійсно дуже складно, так як інформацію, особливо в електронному вигляді, представлено безліччю різних форм. За інформацію можна вважати як базу данних, так і окремий файл, повноцінний програмний комплекс, як і одиничний запис в базі даних. Потрібно розуміти, що всі ці об'єкти можуть піддатися і піддаються атакам зловмисників.

В процесі зберігання, підтримки і надання доступу до будь-якого інформаційного об'єкту його власник, або уповноважена ним особа, накладає явно або самоочевидний набір політик та правил по роботі з нею. Атакою на інформацію класифікується умисне їх порушення. В зв’язку з масовим впровадженням електронно обчислювальних машин (комп’ютерів, смартфонів, мережевих інтерфейсів) в усі сфери людської діяльності кількість інформації, котра зберігається в цифровому вигляді виріс в сотні та тисячі разів. І тепер скопіювати за секунду і віднести флешку з базою даних, що містить

комерційну таємницю, в рази простіше, ніж копіювати або перезаписувати безліч паперів. А з появою комп'ютерних та телекомунікаційних мереж навіть відсутність фізичного доступу до комп'ютерної системи перестало бути гарантією збереження конфіденційності та безпеки інформації

Сучасні методи криптографічного захисту даних є високо ефективними та надійними, використовуючи складні математичні алгоритми для шифрування та захисту інформації від несанкціонованого доступу. Ось деякі з найпоширеніших та важливих методів:

1. Симетричне шифрування: Використовує один ключ для як шифрування, так і розшифрування даних. Алгоритми, такі як AES (Advanced Encryption Standard), DES (Data Encryption Standard) та інші, є популярними методами симетричного шифрування.

2. Асиметричне (публічне) шифрування: Використовує пару ключів: публічний і приватний. RSA, ECC (Elliptic Curve Cryptography) - це відомі алгоритми, які застосовують асиметричне шифрування.

3. Хешування: Використовується для створення унікального хешкоду з вхідних даних. Алгоритми, такі як SHA (Secure Hash Algorithm) та MD5 (Message Digest Algorithm 5), застосовуються для перевірки цілісності даних та підтвердження їхньої автентичності.

4. Цифрові підписи: Використовуються для перевірки автентичності та цілісності даних. Електронні підписи, наприклад, використовують асиметричне шифрування для підтвердження авторства та недоторканності документів.

5. Протоколи обміну ключами: Якісний шифр вимагає безпечного обміну ключами. Протоколи, такі як SSL/TLS, забезпечують захищений обмін ключами для забезпечення безпеки комунікаційних каналів. Сучасні методи криптографічного захисту постійно розвиваються, оскільки з'являються нові загрози та потреби у вдосконаленні захисту. Використання комбінацій різних методів та постійне оновлення криптографічних стандартів є ключовими для забезпечення високого рівня безпеки в обробці та зберіганні даних.

Захист даних став викликом для багатьох сфер, оскільки відбувається масове збереження та обробка інформації в цифровому вигляді. Основний висновок полягає в тому, що захист інформації в цифровому світі вимагає комплексного підходу та постійного вдосконалення методів криптографічного захисту, а також усвідомленням усіма сторонами, як власниками інформації, так і користувачами, про потенційні загрози та важливість захисту конфіденційності й цілісності даних.

Література

1. Борзов Ю. Особливості застосування комп‘ютерного моделювання для покращення навчального процесу / Ю. Борзов, Р. Головатий, Я. Магеровський. // Інформаційні технології розвитку змісту освіти. – 2019. – С. 80–81.

2. Зачко О.Б., Головатий О.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.

УДК 004.056.5

СПОСОБИ ЗАХИСТУ ДАНИХ У ХМАРНОМУ СХОВИЩІ AMAZON S3

Кулик Дмитрій, Горпенюк Андрій
Національний Університет "Львівська політехніка", м. Львів

Анотація: розглянуто заходи щодо гарантування безпеки збереження інформації, включаючи аналіз інноваційних методів та технологій для надійного захисту, які надає хмарне сховище Amazon S3.

Ключові слова: Amazon S3, S3 Bucket, безпека інформації, хмарне сховище.

Annotation: measures to ensure the security of information storage are considered, including an analysis of innovative methods and technologies for reliable protection provided by Amazon S3 cloud storage.

Keywords: Amazon S3, S3 Bucket, information security, cloud storage.

Зберігаючи дані локально, користувач на практиці стикається з рядом проблем: безпека інформації, контроль доступу, масштабування сховища, захист від природніх і техногенних катастроф, тощо. У таких ситуаціях на допомогу приходять хмарні сервіси, один із яких буде розглянуто в цій роботі – Amazon S3 (Simple Storage Service).

S3 – це сервіс для зберігання даних, який пропонує довговічність, доступність, продуктивність, безпеку та, фактично, необмежену масштабованість за дуже низькими цінами, що робить його неабияк популярним серед користувачів. Головним об'єктом у ньому є Bucket'и, які виступають у ролі сховища для інформації.

Зрозуміло, коли йдеться про збереження інформації, питання її захищеності стоїть дуже гостро. Зважаючи на це, сервіс S3 пропонує різноманітні безпекові рішення із використанням найкращих практик.

Важливим аспектом безпеки інформації є те, хто має права на доступ до неї та яким чином ці політики створюються та впроваджуються. За це в S3 відповідає bucket policy. Bucket policy – це політика на основі ресурсів, яку можна використовувати для надання дозволів на доступ до S3 bucket'а та об'єктів у ньому. Дозволи, додані до bucket'а, застосовуються до всіх об'єктів (наявних і будь-яких нових у подальшому), які там зберігаються. У такий спосіб забезпечується повний контроль над тим, хто, які дії та за яких умов може або не може виконувати. Для прикладу нижче наведено bucket policy, яка забороняє будь які дії над об'єктами, якщо запит походить не з конкретно визначеного діапазону IP-адрес (рис. 1).

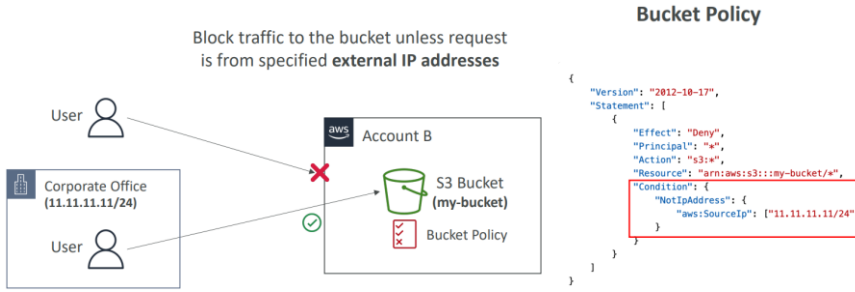


Рисунок 1 – приклад застосування bucket policy для обмеження доступу

Захист даних означає їхню безпеку під час передачі (переміщення до та з Amazon S3) і в стані спокою (під час зберігання на дисках в Amazon S3 дата-центрі). Щоб захистити дані, що перебувають у спокої (at rest), хмарне сховище надає можливість шифрування на стороні сервера – Amazon S3 шифрує об'єкти перед збереженням на дисках у дата-центрах AWS, а потім розшифровує об'єкти при їх завантаженні. Для всіх bucket'ів Amazon S3 за замовчуванням налаштовано шифрування, і всі нові об'єкти, які завантажуються в S3 bucket, автоматично шифруються в стані спокою. Шифрування на стороні сервера за допомогою керованих ключів Amazon S3 (SSE-S3) є конфігурацією шифрування за замовчуванням для кожного bucket'а в Amazon S3. До цього ж, на вибір надаються чотири взаємовиключні варіанти шифрування на стороні сервера, залежно від способу керування ключами шифрування та кількості рівнів шифрування, які потрібно застосувати.

Так як ми розглядаємо хмарне сховище, то зрозуміло, що взаємодія з об'єктами теж має проводитися безпечним шляхом. Тут у нагоді стає bucket policy. Наприклад, ми можемо заборонити доступ до об'єктів всередині bucket'а, якщо запит надходить по незахищеному з'єднанню (рис. 2).

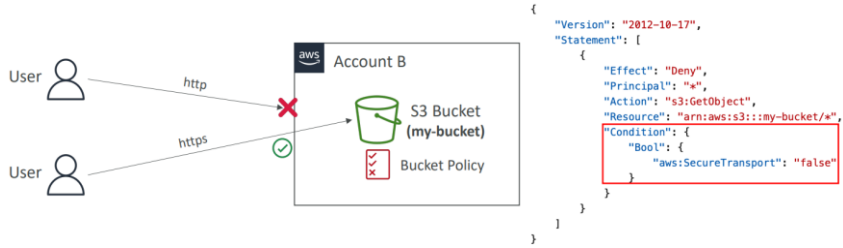


Рисунок 2 – приклад застосування bucket policy для заборони отримування об'єктів по незахищеному з'єднанню

Мабуть, ніхто б не хотів, щоб їхня інформація потрапила в публічний доступ. Спеціально для таких ситуацій S3 пропонує ряд налаштувань для блокування публічного доступу до bucket'а (рис. 3). Вони були створені для запобігання витоку даних у компаній.

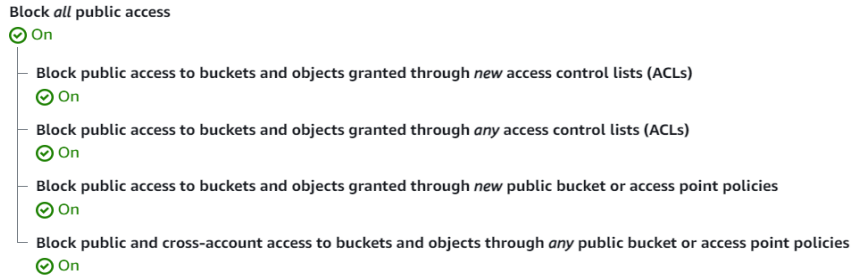


Рисунок 3 – налаштування для блокування публічного доступу до bucket'а

Достатньо важливо захистити інформацію від (не)навмисного видалення. В S3 із цим допомагає Versioning (керування версіями). Завантаження одного і того ж файлу із різним вмістом просто створить відповідні версії в bucket'і. Такий функціонал також дуже зручний для випадків, коли є потреба повернутися до однієї з попередніх версій файлу. Як додатковий рівень захисту, S3 ще пропонує MFA Delete – примушувати користувачів генерувати код на пристрої (зазвичай мобільному телефоні чи апаратному засобі) перед виконанням важливих операцій на S3 (остаточне видалення версії об'єкту та призупинення керування версіями).

Отже, дослідження підтверджує, що хмарні сховища, зокрема Amazon S3, є перспективним та ефективним рішенням для зберігання даних. Проте, важливо враховувати, що належне гарантування безпеки інформації в цих сервісах вимагає глибокого розуміння та використання заходів захисту даних, щоб уникнути потенційних ризиків і забезпечити надійність, цілісність і конфіденційність інформації користувачів.

Література

1. Stephane Maarek. Ultimate AWS Certified Security Specialty [NEW 2023] SCS-C02 [Електронний ресурс]. – Режим доступу : URL : https://www.udemy.com/course/ultimate-aws-certified-security-specialty/.

2. Stephane Maarek. Ultimate AWS Certified Solutions Architect Associate SAA-C03 [Електронний ресурс]. – Режим доступу : URL : https://www.udemy.com/course/aws-certified-solutions-architect-associate-saa-c03/.

3. What is Amazon S3? – Amazon Simple Storage Service [Електронний ресурс]. – Режим доступу : URL : https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html.

УДК 004.056.57

ЗАСТОСУВАННЯ ВІРТУАЛЬНОГО СЕРЕДОВИЩА ДЛЯ ДОСЛІДЖЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Кутник Назар, Маслова Наталія
Львівський державний університет безпеки життєдіяльності, Львів

Анотація: Шкідливе програмне забезпечення може завдати шкоди комп'ютерній системі різними способами, як то заблокувати роботу; зашифрувати або видалити дані; викрасти конфіденційну інформацію; використати пристрій для проведення масштабних вірусних атак. Сучасним підходом й одним з способів дослідження підозрілого програмного забезпечення є його аналіз у спеціально створеному віртуальному середовищі.

Ключові слова: шкідливе програмне забезпечення, вірус, віртуальне середовище.

Abstract: Malware can harm a computer system in a number of ways, such as blocking operations; encrypt or delete data; steal confidential information; use the device to carry out large-scale virus attacks. A modern approach and one of the ways to investigate suspicious software is its analysis in a specially created virtual environment.

Keywords: malware, virus, virtual environment.

Для аналізу роботи та характеристик шкідливого програмного забезпечення, оцінювання його впливу на комп'ютерну систему застосовують різні методи, як то статичний, динамічний аналіз, дослідження коду та змісту оперативної пам'яті. Виявлення потенційно шкідливого програмного забезпечення вимагає спеціального, безпечного та надійного тестового середовища.

Метою даної роботи є опис розгортання тестового середовища й демонстрація результату запуску шкідливого програмного забезпечення в створеній віртуальній системі.

Шкідливе або підозріле програмне забезпечення може принести шкоду комп'ютеру користувача, заблокувати або порушити його роботу, викрасти дані. Щоб унеможливити проникнення шкідливого програмного забезпечення в основну систему, створюється й налагоджується віртуальне тестове середовище [1].

Одним з методів є створення під управлінням Ubuntu Linux хост-машини з екземплярами віртуальних машин Ubuntu Linux VM та Windows. Віртуальні машини налаштовуються як частина однієї мережі, між ними організовується обмін інформацією. Щоб шкідливий контент не витік в інтернет та на основний комп'ютер, використовується режим конфігурації мережі host-only. При створенні середовища встановлювались: система керування пакетами (pip), утиліта для моделювання різних інтернет-служб

(INetSim), пакет Wireshark для аналізу мережного трафіку, окремі утиліти Python та спеціалізовані бібліотеки (у тому числі - бібліотеку YARA). YARA може використовуватись для виявлення сигнатур шкідливих файлів й не тільки виявляти шкідливий контент, але й ідентифікувати й класифікувати файли, якщо вони мають однакові або схожі характеристики. Процес настроювання й встановлення експериментального віртуального середовища наведено на рисунку 1.

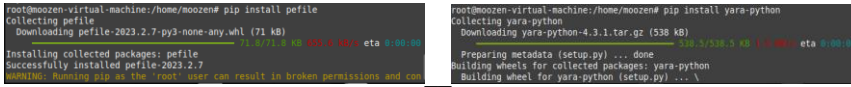


Рисунок 1 – Встановлення віртуальної машини та yara-python

Приклад шкідливого контенту було взято з сайту http://vxvault.net/ViriList.php, але робота з сайтом в даний момент є безпечною, що підтверджено процедурою аналізу шкідливого контенту Malware Analysis [2].

Не дивлячись на те, що код вірусу, який досліджується, був раніше знезараженим, у віртуальному середовищі зловмисне програмне забезпечення активізувалося, що підтверджується появою повідомлення-вимоги й блокуванням роботи віртуального середовища. Повідомлення – підтвердження роботи вірусного програмного забезпечення продемонстровано на рисунку 2 показано.

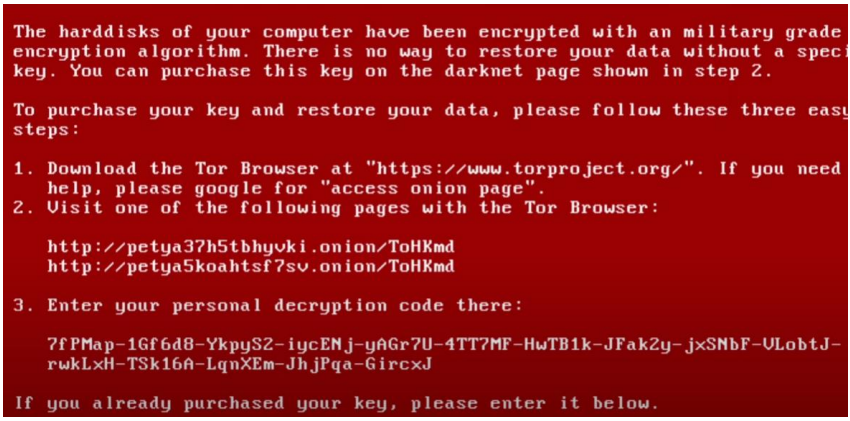


Рисунок 2 – Повідомлення вірусу – вимагання грошей за ключ доступу

Шкідливим програмним забезпеченням, знайденим на інтернет-сайті, виявився вірус-вимагач, вірус-шантажист, ransomware. Програми-вимагачі – це різновид зловмисного програмного забезпечення, яке зазви-

чай блокує доступ користувача до свого комп'ютера, шифрує дані (часто застосовні алгоритми – AES та RSA), а потім вимагає грошовий викуп за відновлення доступу [3]. Розповсюдженими шляхами проникнення програм-вимагачів на комп'ютер жертви є електронні листи зі шкідливим вкладенням, впровадження зловмисного коду у веб-сторінки, створення переадресувань на шкідливі сайти.

Видалення такого вірусу не є простою задачею, його архітектура передбачає прив'язку до бібліотек операційної системи, користувацьких програм, блокування екрану, портів, й інші зловмисні дії [4]. Система безпеки Microsoft Windows має засоби видалення зловмисних програм типу ransomware, але в динамічному режимі відбувається виявлення та блокування шкідливого коду, а остаточне видалення – при повторному запуску системи.

В експерименті, який описується, шкідливу програму було запущено у віртуальному середовищі системи Windows, а віртуальна машина Linux використовувалась для моніторингу мережного трафіку та була налаштована на моделювання інтернет-сервісів (DNS, HTTP тощо), щоб забезпечити належну відповідь, коли шкідлива програма буде запитувати їх.

Шкідливий контент успішно адаптувався в віртуальному середовищі, почав працювати, що привело до блокування роботи низки системних ресурсів, появи екрану з повідомленням вірусу з вимаганням грошей за ключ доступу й порушенню роботи віртуальних систем.

Проведений експеримент підтвердив необхідність уважного ставлення до виконання робіт з аналізу шкідливого програмного забезпечення, навіть, якщо його код є відомим й зафіксованим на спеціальних ресурсах, доречність розгортання спеціального віртуального середовища для дослідження й аналізу шкідливого або підозрілого контенту.

Література

1. Monnappa K A, Learning Malware Analysis: Packt Publishing Ltd., 2018., 501 p.

2. AnyRun Аналіз шкідливих програм. Interactive Malware Analysis. URL: https://any.run/report/a82b6cfe1ca1bf3b30652b52c438d74c4

3. Ransomware. URL: https://www.enigmasoftware.com/threat-database/ransomware/

4. Шифрувальники-вимагачі (ransomware): приклади та тенденції у 2023. URL: https://gridinsoft.ua/ransomware

УДК 004.7

СТРАТЕГІЇ ПОБУДОВИ CYBER SECURITY OPERATION CENTER (CSOC)

Ліщинська Мар'яна, Дмитрович Анастасія
Львівський національний університет імені Івана Франка

Анотація: CSOC – команда спеціалістів кібербезпеки, яка займається моніторингом та аналізом безпеки організації під час реагування на потенційні чи поточні інциденти. Вона можуть включати в себе і спеціалістів з суміжних команд, наприклад CERT і бути частиною SOC. Відповідно до розмірів і потреб організації існує 9 моделей побудови CSOC.

Ключові слова: CSOC, Security operation center (SOC), Computer Emergency Response Team (CERT), Централізований CSOC, Організація, Модель, Ad Hoc Security Response, Security as Additional Duty, Distributed SOC, Centralized SOC, Ієрархічний CSOC, Федеративний і Національний та Координуючий CSOC, Managed Security/SOC Service Provider (MSSP), Ділова потреба, Рівень ризику, Місія CSOC, Situational Awareness, Подія, Інцинент.

CSOC може імплементувати в свою структуру такі категорії функцій:

− Incident Triage, Analysis and Response – категорія властивостей і функцій, яка допомагає аналітикам відокремити потенційні надзвичайні ситуації від звичайних потреб реагування. Тобто відокремити події від інцидентів, і якщо стався інцидент, зреагувати на нього. Подія відрізняється від інциденту тим, що вона потребує дослідження аналітика, а інцидент може бути виявлений аналітиком або його видно в мережі, тобто виконується зловмисна діяльність і інцидент потребує реагування.

− Cyber Threat Intelligence, Hunting, and Analytics – функції, як спрямовані на обробку загроз. Увага зосереджується на діях зловмисника, а не на спостереженні за активами організації. Діяльність фокусується на розслідуванні інцидентів та реагуванні на них під час критичних ситуацій та значних порушень.

− Expanded SOC Operations – розширений інструментарій SOC, який допомагає аналітикам краще орієнтуватися на зловмисника.

− Vulnerability Management - це безперервний регулярний процес виявлення, оцінювання, звітування, керування та усунення кіберврразливостей у системах, якими володіє організація.

− SOC Tools, Architecture, and Engineering – категорія, яка описує інструменти, які зазвичай використовує SOC в роботі аналітиків кібербезпеки. Наприклад EDR, SIEM, SOAR.

− Situational Awareness, Communications, and Training – можливість навчати персонал.

− Leadership and Management – категорія властивостей, яка включає в себе правильний розподіл персоналу на ту чи іншу посаду.

Література

1. Kathryn Knerler, Ingrid Parker, Carson Zimmerman 11 strategies of world-class cybersecurity operations center/ Kathryn Knerler, Ingrid Parker, Carson Zimmerman, 2022. – 452p.

УДК 004.7

ДОСЛІДЖЕННЯ ТЕХНІК І ТАКТИКИ, ЯКІ ВИКОРИСТОВУЮТЬСЯ ПРИ КІБЕРАТАКАХ, БАЗУЮЧИСЬ НА MITRE ATT&CK MATRIX

Ліщинська Мар'яна, Дмитрович Анастасія
Львівський національний університет імені Івана Франка

Анотація: захист організації це завжди необхідність, яку не можна упускати. Саме тому, ця робота є спрямованою на повне дослідження незмінного інструменту, що допомагає захистити дані та комп`ютерні системи. На практичному застосуванні, я показала, як швидко відбувається потенційний напад із боку атакуючого та як покроково можна його відслідкувати спираючись на техніки та тактики Mitre ATT&CK Matrix.

Ключові слова: MITRE ATT&CK MATRIX, техніка, тактика, атака, EternalBlue, WannaCry, MS17-010, вразливість, кібератака, протоколі SMBv1, авторизація, віддалене виконання коду, Initial Access, Credential Access, Credential Dumping, Lateral Movement, Server Message Block, Exfiltration, VPN, CNC, порт 445, база даних, зловмисники.

Розглянемо на практиці, як виглядає використання технік і тактик, базуючись на MITRE ATT&CK Matrix. На рисунку 1 зображено приклад атаки MS17-010, також відомої, як EternalBlue. Вона є однією із вразливостей, яка була використана у великому масштабі під час кібератаки WannaCry у 2017 році.Ця атака використовується для експлуатації вразливості в протоколі SMBv1 (Server Message Block version 1), який використовується для обміну файлами та принтерами в мережах Windows. Основним використанням атаки MS17-010 є віддалене виконання коду без авторизації, що дозволяє зловмисникам захопити управління над цільовим комп'ютером. Для успішної атаки зловмиснику потрібно мати доступ до мережі, в якій знаходиться цільовий комп'ютер, і використовувати експлойт EternalBlue. Продемонструємо детальний аналіз атаки використовуючи техніки і тактики MITRE ATT&CK Matrix. На рисунку 1 ми можемо побачити, що є 4 фази, які є кроками атаки.

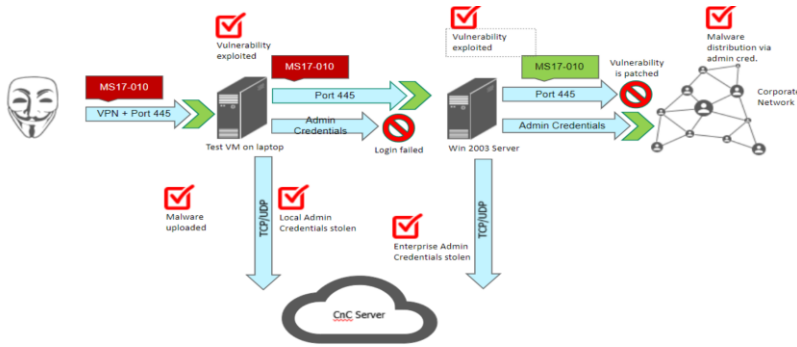


Рисунок 1

На рисунку 2 чітко показано, де саме є потенційні фази атаки.

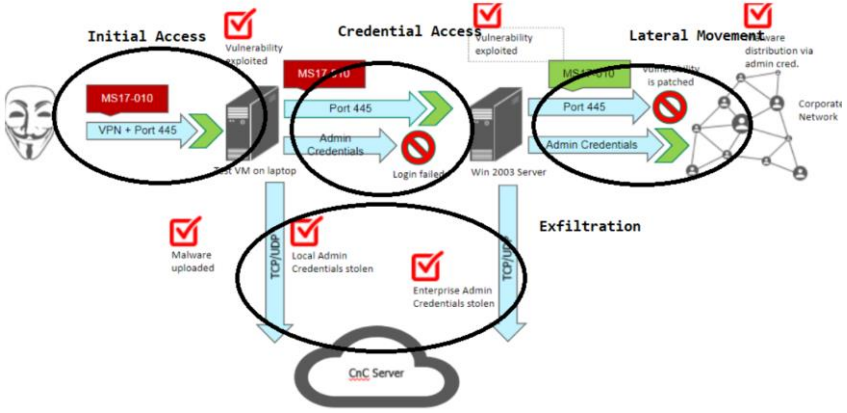


Рисунок 2

У першій фазі атаки відбувається застосування техніки Initial Access (Початковий доступ). Зловмиснику вдається отримати початковий доступ до віртуальної машини (Test VM) на ноутбуці через використання VPN та порту 445. Атакуючі базуються на тактику Exploit Public-Facing Application (Експлуатація загальнодоступної програми). Вони можуть використовувати вразливості в загальнодоступних програмах або сервісах, таких як сервер SMB (порт 445), щоб отримати несанкціонований доступ. У другій фазі злочинці намагаються використати техніку Credential Access (Доступ до облікових даних): Зловмисник намагається отримати доступ до адміністративних облікових даних на сервері Windows 2003 (Win 2003 Server). Атакуючі базуються на тактику Credential Dumping (Отримання облікових даних). Вони можуть використовувати методи для отримання облікових даних зі зламаних або компрометованих систем. Це може включати використання інструментів для витягування паролів з оперативної пам'яті, крадіжку хешів паролів або перехоплення облікових даних під час процесу аутентифікації.

У третій фазі зловмисники використовують техніку Lateral Movement. Це є етапом атаки, коли зловмисники рухаються по внутрішній мережі після отримання початкового доступу, з метою пошуку інших систем для компрометації та подальшої ескалації атаки. Відповідно до нашої атаки, зловмиснк використовує протокол SMB(Server Message Block), який включає порт 445, для пошуку інших систем у мережі. Вони можуть сканувати підмережі або використовувати інші методи, щоб виявити інші системи. У заключному етапі відбувається викрадення даних (Exfiltration). В контексті атаки MS17-010 з використанням доступу через VPN по порту, зловмисники відправляють вкрадені дані на CnC сервер. Це може включати відправку файлів, баз даних або іншої конфіденційної інформації через зашифрований канал до CNC сервера.

Отже, на прикладі атаки EternalBlue було зображено та проаналізовано на основі MITRE ATT&CK Matrix, як на практиці зловмисник доступається до даних та викрадає їх.

Література

1. Офіційний веб-сайт Mitre ATT&CK [Електронний ресурс]: https://attack.mitre.org/
2. MITRE Cybersecurity Insights: MITRE Cybersecurity Insights [Електронний ресурс]:
https://www.mitre.org/cybersecurity/insights
3. What is MITRE ATT&CK? [Електронний ресурс]: https://www.vmware.com/topics/glossary/content/mitre-attack.html
4. How to use the MITRE ATT&CK Framework [Електронний ресурс]:https://www.chaossearch.io/blog/how-to-use-mitre-attck-framework

УДК 004.738.522

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ SIEM-СИСТЕМ В МЕНЕДЖМЕНТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Логойда Ярослав, Ящук Валентина, Фединець Наталія
Львівський державний університет безпеки життєдіяльності, Львів, Україна

Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи використання SIEM-систем в менеджменті інформаційної безпеки. Визначено сучасні підходи до управління інформаційною безпекою та розслідування інцидентів. Наведено методичні підходи до формування концепції функціонування SIEM-систем в менеджменті інформаційної безпеки. Запропоновано етапи вирішення науково-практичної проблеми, пов'язаної з підвищенням рівня захисту інформаційних систем з використанням SIEM-систем в менеджменті інформаційної безпеки.

Ключові слова: інформаційна безпека, менеджмент інформаційної безпеки, SIEM-системи.

The theoretical, scientific-methodical and organizational-functional bases of using SIEM systems in information security management are considered. Modern approaches to information security management and incident investigation are defined. Methodical approaches to the formation of the concept of operation of SIEM systems in information security management are given. The stages of solving the scientific and practical problem associated with increasing the level of protection of information systems using SIEM systems in information security management are proposed.

Keywords: information security, information security management, SIEM systems.

Сучасні інформаційні системи та мережі все більше уразливі до різноманітних загроз, таких як несанкціонований доступ, розкрадання інформації, DDoS-атаки, інвазії шкідливого програмного забезпечення та інші. Ці загрози стають все більш складними і витонченими, що ускладнює їх виявлення та запобігання. Сучасні організації використовують складні інформаційні системи та мережі, які включають в себе різноманітні пристрої, додатки та протоколи. Для забезпечення ефективного управління інформаційною безпекою необхідно мати всебічний огляд всіх компонентів інформаційної системи. Управління інформаційною безпекою є складним і трудомістким завданням, яке вимагає постійного моніторингу та аналізу великої кількості даних. SIEM системи дозволяють автоматизувати багато завдань безпеки, що звільняє персонал для виконання інших важливих завдань. Зважаючи на це актуальність використання SIEM систем в менеджменті інформаційної безпеки є незаперечною.

SIEM-система – це система управління інформаційною безпекою та розслідуванням інцидентів (Security Information and Event Management). Вона призначена для збору, консолідації, зберігання, аналізу та візуалізації даних безпеки з різних джерел, таких як мережеві пристрої, сервери, робочі станції, програмне забезпечення безпеки тощо. SIEM-системи використовуються для виявлення, реагування та розслідування інцидентів безпеки, а також для забезпечення відповідності вимогам безпеки. SIEM-система (Security Information and Event Management) - це програмне забезпечення, яке збирає, обробляє та аналізує дані про події безпеки з різних джерел, таких як мережеві пристрої, сервери, додатки та кінцеві точки. SIEM-системи використовуються для виявлення, реагування та запобігання загрозам інформаційній безпеці.

Робота SIEM-системи можна розділити на чотири основних етапи: збір даних; консолідація та зберігання даних; аналіз даних; розробка звітів та сповіщень. Окрім цих основних етапів, SIEM-система може виконувати також інші функції, такі як: менеджмент відповідей на інциденти – допомога в реагуванні на виявлені інциденти; аналіз поведінки користувачів – виявлення аномалій у поведінці користувачів; відстеження відповідності вимогам – забезпечення відповідності вимогам безпеки. Етапи роботи SIEM-системи можуть бути адаптовані до конкретних потреб організації. Наприклад, організація, яка має обмежений бюджет, може зосередитися на основних етапах, таких як збір, консолідація та зберігання даних. А організація, яка має високий рівень ризику, може використовувати більш складні функції, такі як аналіз поведінки користувачів або управління відповідями на інциденти.

SIEM-системи збирають дані з різних джерел, таких як: мережеві пристрої, такі як брандмауери, маршрутизатори, комутатори тощо; сервери, такі як веб-сервери, файлові сервери, бази даних тощо; робочі станції, такі як комп'ютери, ноутбуки, планшети тощо; програмне забезпечення безпеки, таке як антивірусні програми, системи виявлення вторгнень (IDS), системи управління вразливостями тощо. SIEM-системи можуть збирати дані в різних форматах, таких як текстові файли, XML, JSON, CSV тощо. SIEM-система повинна мати можливість обробляти та перетворювати дані в єдиний формат для подальшого аналізу.

SIEM-системи можуть збирати дані кількома способами, такими як: пряме підключення – SIEM-система може підключатися безпосередньо до джерела даних і отримувати дані в реальному час; сервер повідомлень – SIEM-система може отримувати дані з сервера повідомлень, який збирає дані з різних джерел; автоматичне завантаження – SIEM-система може автоматично завантажувати дані з локальних або віддалених файлів; вибір методу збору даних залежить від конкретного джерела даних і потреб організації.

Основними функціями SIEM-систем є збір даних, обробка даних, фільтрація, кореляція, аналіз, виявлення аномалій, виявлення вторгнень,

виявлення загроз, генегація рішень, повідомлення про загрози, автоматичне реагування. Сьогодні на світовому ринку представлено широкий спектр SIEM-систем, які пропонують різні функції та можливості. Ось деякі з найпопулярніших сучасних SIEM-систем:

- IBM QRadar: Комплексна SIEM-система, яка пропонує широкий спектр функцій, включаючи виявлення вторгнень, аналіз загроз, управління інцидентами та реагування на них.
- Splunk Enterprise Security: SIEM-система, яка спеціалізується на аналізі великих обсягів даних.
- Microsoft Sentinel: SIEM-система, яка інтегрована з іншими продуктами Microsoft, такими як Azure Monitor та Azure Security Center.
- Siemplify: SIEM-система, яка пропонує простий і зручний інтерфейс.
- LogRhythm: SIEM-система, яка пропонує широкий спектр функцій та можливостей для великих організацій.

При виборі SIEM-системи слід враховувати такі фактори, як: розмір організації, типи даних, які потрібно збирати, функції та можливості, які потрібні. SIEM системи є ефективним інструментом для підвищення рівня інформаційної безпеки організації. Вони допомагають організаціям виявити потенційні загрози на ранніх стадіях, забезпечити відповідність вимогам безпеки, зменшити час реагування на інциденти безпеки та покращити ефективність управління інформаційною безпекою.

Література

1. Кошара, А. Підвищення захищеності державного сектору на основі SIEM-систем. // Кошара, А., Бакало, Б. / Інфокомунікаційні та комп'ютерні технології, 2(04), (2023). 128-133. [Електронний ресурс]. – Режим доступу: https://doi.org/10.36994/2788-5518-2022-02-04-14

2. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю.Драб, В. Ящук // 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 004.4

РОЗРОБКА СПАМ-ФІЛЬТРУ З ВИКОРИСТАННЯМ AI/ML

Макарова А.М.
Національний університет "Одеська політехніка", Україна

Цю роботу присвячено розробці спам-фільтра з використанням технологій штучного інтелекту та машинного навчання. У роботі розглядаються наявні методи фільтрації, аналізуються можливості інтеграції з поштовими сервісами та розглядаються ключові етапи розробки та забезпечення безпеки даних.

This paper is devoted to the development of a spam filter using artificial intelligence and machine learning technologies. The paper reviews existing filtering methods, analyses the possibilities of integration with email services and considers the key stages of development and data security.

Вступ. Спам-фільтри відіграють критичну роль у забезпеченні безпеки електронної пошти, запобігаючи загрозам безпеці, пов'язаним із фішингом, вірусами та шахрайством. Для користувачів вони стають засобом підвищення ефективності та зручності використання електронної пошти, а для організацій – невід'ємною частиною загальної стратегії інформаційної безпеки [1].

Мета роботи. Метою цього дослідження є розробка ефективного спам-фільтра, що використовує технології штучного інтелекту та машинного навчання для забезпечення високого ступеня захисту від небажаних повідомлень.

Основна частина роботи. Для розробки програми фільтрації спаму із використанням машинного навчання необхідно вивчити існуючі методи та концепції машинного аналізу тексту, такі як аналіз частин мови, визначення ключових слів і аналіз частоти. Потрібно обрати інструменти машинного навчання та зібрати розмічені дані – набори електронних листів, відмічених як спам та не спам. Далі слід розробити та навчити модель, використовуючи алгоритми (наївний класифікатор Байєса, машина опорних векторів *SVM*, глибокі нейронні мережі). Важливо розглянути опції інтеграції з електронною поштою. Після цього протестувати модель на нових даних. Окрема увага має бути приділена безпеці даних при обробці електронних листів, забезпечуючи захист особистих даних користувачів.

Програмне забезпечення для фільтрації спаму, як правило, надається у вигляді спеціалізованих рішень, які розгортаються на серверах електронної пошти або інтегруються у хмарні поштові служби. Встановлюється на поштовому сервері або у хмарному середовищі для обробки вхідного та/або вихідного поштового трафіку. Адміністратор налаштовує параметри та правила фільтрації, а програмне забезпечення регулярно оновлюється

для забезпечення актуальних правил та алгоритмів. Спам-фільтр використовує різні технології, такі як байєсівський фільтр та *ML*, для аналізу кожного повідомлення. Позначені спам-повідомлення можуть бути перенаправлені, позначені або видалені згідно з налаштуваннями. Адміністратор виправляє хибні спрацювання та моніторить ефективність через звітність. Спам-фільтри працюють у фоновому режимі, оброблюючи трафік без втручання користувачів.

Рішення для фільтрації спаму, орієнтовані на підприємства, інтегруються з різними поштовими серверами, такими як *Microsoft Exchange, Office 365, Google Workspace*. Взаємодія може відбуватись через API, надані багатьма поштовими серверами, наприклад, *EWS (Microsoft Exchange)* або *Gmail API*. Альтернативний варіант – створення поштового проксі для перехоплення трафіку між клієнтом і сервером для аналізу та фільтрації. Інтеграція може використовувати стандартні поштові протоколи *(IMAP, POP3, SMTP)* для взаємодії з різними серверами. Можуть бути розроблені плагіни для популярних поштових клієнтів, надаючи додаткові функції фільтрації. Також може бути надано *API* чи *SDK*.

У ході проектування були розглянуті популярні аналоги-додатки для фільтрування спаму: *SpamAssassin, Proofpoint, Sophos Email Security, Symantec Email Security*. Результати досліджень наведено у таблиці 1.

Таблиця 1 – Порівняльні характеристики продуктів-аналогів

Критерій	*SpamAssassin*	*Proofpoint*	*Sophos Email Security*	*Symantec Email Security*
Ціна	Безкоштовно	Підписка	Підписка + *trial period*	Підписка
Користувачі	Організації будь-якого масштабу по всьому світу.	Різні організації, включно з великими підприємствами та органами держ. влади.	Організації різного масштабу.	Широкий спектр клієнтів, від невеликих підприємств до великих корпорацій.
Платформи	Різні ОС (включ. *Linux* і *Unix*-подібні).	Доступний як хмарне рішення (*SaaS*) і як ПЗ для розгортання всередині підприємств.	Надається як хмарне рішення (*Sophos Central*) і як ПЗ для самостійного розгортання.	Надається як хмарне рішення і для розгортання всередині підприємств.
Осн. функціонал	Фільтр спаму з використ. байєсівського аналізу, перевірка заголовків, аналіз вмісту, використ. чорних та	Захист від спаму, фішингу та шкідливих вкладень. Включає аналіз поведінки, технології *ML*, контроль *URL*.	Захист від спаму, фішингу, антивірусний захист, аналіз вкладень, технології машинного навчання, хмарна архі-	Антивірусний захист, фільтрація спаму, аналіз поведінки, аналіз вмісту, захист від фішингу, технології *ML*.

	білих списків.		тектура.	
UI/UX	Зазвичай налаштовується і керується через конфігураційні файли. Інтерфейс командного рядка, не має *GUI*.	Володіє великим веб-інтерфейсом з детальними панелями адміністратора і функц. для кінцевих користувачів.	Має інтуїтивно зрозумілий веб-інтерфейс для адміністраторів із підтримкою різних функцій і налаштувань.	Має деталізований веб-інтерфейс із безліччю опцій конфігурації та звітності.
Переваги	Розширюваність і настроюваність. Велика спільнота.	Масштабованість, хмарні рішення, розширені функції безпеки, аналітика.	Простота використ.. Безліч функцій безпеки. Хмарні та локальні варіанти.	Масштабованість. Аналіз поведінки. Безліч функцій безпеки.
Недоліки	Потребує досвіду в налашт. та обслуговування. Може вимагати додаткові інстр. для макс. ефективності.	Платне рішення може бути дорогим для невеликих підприємств.	Можуть виникнути додаткові витрати на оновлення та підтримку.	Висока вартість.

Можливості розширення та інтеграції програми-спам-фільтра включають безпечну передачу даних з використанням шифрування (*SSL/TLS*) для взаємодії з поштовими серверами чи клієнтами. Також можна запровадити механізми аутентифікації для безпечного доступу до поштових систем. Розширення функціоналу для аналізу вкладень в електронних повідомленнях для виявлення вірусів або інших загроз є однією з опцій. Додавання звітних механізмів для відстеження та аналізу ефективності фільтрації також може бути корисним. Можна надати можливість налаштовувати фільтрацію через інтерфейс додатку або *API*.

Висновки. У роботі розглянуто розробку спам-фільтра з використанням штучного інтелекту та машинного навчання. Визначено ключові етапи розробки, проведено аналіз можливостей інтеграції з поштовими сервісами та підкреслено важливість забезпечення безпеки даних. Розглянуто аналоги-додатки для фільтрації спаму, а також висвітлено можливості розширення та інтеграції додатку спам-фільтра.

Література

1. Аналіз та обґрунтування проекту для фільтрування спаму з використанням AI/ML / Д. С. Шибаєв, М. Д. Рудніченко, М. О. Кузнєцов, Мірей Мбойя // Project, Program, Portfolio p3 management : третя Міжнарод. наук.-практ. конф. : тези доп., м. Одеса, 07–08 груд. 2018 р. / Одес. нац. політехн. ун-т. – Одеса, 2018. – Т. 2. – С. 117–118.

УДК 004.415.24

РОЗВИТОК Й ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ ТА СТЕНОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНОМУ СВІТІ

Малець Остап-Святослав, Смотр Ольга
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Цей допис описує основні способи та причини використання стеганографії у сучасному світі. Способи створення стеганографічних шифрів, галузі застосування, та майбутнє цього методу шифрування даних.
***Ключові слова*:** захист інформації, стеганографія, криптографія, інформаційні війни.

This post outlines the fundamental methods and reasons for the use of steganography in the modern world. It discusses the creation of steganographic ciphers, the scope of their application, and the future of this method of data encryption.
Keywords: information security, steganography, cryptography, information warfare.

Інформація завжди була “на вагу золота”. Та чи інша інформація, або ж її відсутність може врятувати, або ж погубити тисячі життів за лічені секунди, принести мільйони, або ж загубити все ваше майно. У поточному світі, захист такої інформації стає майже одним з найважливіших завдань яке постає перед людьми різних професій від військових, до авторів музичних творів.

Стеганографія – це наука або мистецтво приховування інформації в інших даних таким чином, щоб її наявність залишалася непоміченою або малоймовірною. У відміну від криптографії, де мета полягає у забезпеченні конфіденційності, ціллю стеганографії є збереження факту самого існування прихованої інформації. Стеганографія включає в себе різноманітні методи, такі як приховування тексту у зображеннях, аудіофайлах або інших носіях інформації. Цей підхід дозволяє передавати конфіденційну інформацію, не викликаючи підозрюваності, оскільки сам факт приховування залишається непоміченим.

Криптографія – це наука про забезпечення конфіденційності, цілісності та автентичності інформації за допомогою застосування математичних та алгоритмічних методів. Основна мета криптографії - забезпечити безпеку передачі і зберігання інформації, так щоб тільки авторизовані особи мали доступ до неї.

Мистецтво приховання інформації в видимо невинних даних, знаходить своє застосування у різних контекстах завдяки своїй багатогранній корисності. Індивіди та організації використовують стеганографію з різних причин, починаючи від захисту конфіденційної інформації та забезпечення безпеки даних до менш очевидних застосувань, таких як шпигунство чи

кібервійна. Розвідувальні агентства можуть використовувати стеганографічні техніки для приховування конфіденційних повідомлень у цифрових медіаданих, тим самим зменшуючи ризик виявлення. Також індивіди, які прагнуть захистити свою конфіденційність або передавати інформацію непомітно, можуть також користуватися стеганографією. Поза сферою безпеки та прихованого зв'язку стеганографія слугує практичним цілям, таким як цифрове водяне знакування та захист авторських прав, що дозволяє ідентифікувати та зберігати інтелектуальну власність. З розвитком технологій застосування стеганографії продовжують розширюватися, що вимагає належних засобів кібербезпеки та постійних досліджень для протидії можливому зловживанню.

У сучасному світі стеганографія знаходить реальне застосування в різних сферах, включаючи кібербезпеку та розвідку. Наприклад, в 2019 році було виявлено, що хакерська група DarkHydrus використовує стеганографію для приховання своїх зловмисних дій. Вони вбудовували свої атаки у безпідозренні файли з зображеннями та документами, щоб уникнути виявлення та блокування їхніх зловмисних дій системами безпеки. Також, у 2020 році стало відомо про використання стеганографії в атаках на мобільні пристрої. Зловмисники вбудовували шкідливий код у зображення, які виглядали як беззаперечні файли, але містили прихований код для атаки на операційні системи пристроїв. Ці приклади свідчать про те, як стеганографія використовується для обхіду захисту та збереження конфіденційності при виконанні цифрових атак.

Також стеганографія знайшла застосування і у військовій сфері. Цей метод забезпечує можливість таємного обміну інформацією, що стає критичним у воєнний період. Інтеграція конфіденційної інформації у "невинно виглядаючі" файли чи повідомлення може допомогти уникнути її виявлення противником та зберегти стратегічну перевагу. Також використання даної технології можливе для приховування слідів та обману ворожих розвідників. Цей метод може ускладнити виявлення та аналіз важливих воєнних даних, тим самим зберігаючи стратегічні секрети та забезпечуючи додатковий рівень безпеки під час конфлікту.

Підсумовуючи, можна сказати що зараз дуже важливо слідкувати за розвитком цієї сфери через постійне зростання її застосування та потенційних викликів, які вона створює для кібербезпеки. Спільно зі зростанням обсягів цифрової інформації та її обміну, стеганографія набуває нового значення як засіб конфіденційного зв'язку та приховання даних. З одного боку, це може бути використано для захисту особистої приватності та конфіденційності в цифровому середовищі. З іншого боку, технологічний прогрес у цьому напрямку може послужити інструментом для кіберзлочинців та шпигунів, які шукають нові методи обходу безпекових заходів. Відповідно, слідкування за розвитком стеганографії є важливим для розуміння та ефективного протидії потенційним кіберзагрозам, а також для розвитку більш сучасних та ефективних методів кібербезпеки.

Література

1. Nicholas J Hopper, John Langford and Luis Von Ahn, Provably Secure Steganography
2. Neil F Johnson, An Introduction to Watermark recovery from Images
3. Niels Provos, Defending against Statistical Steganlysis
4. Karen Su, Deepa Kundur and Dmitrios Hatzinakoa, A novel approach to collusion resistant Video watermarking.

ОГЛЯД ФУНДАМЕНТАЛЬНОЇ МОДЕЛІ "АВТОМАТИЗОВАНОЇ КОНЦЕПЦІЇ ПЕРЕВІРКИ ВІДПОВІДНОСТІ СТАНДАРТАМ" ЩОДО БЕЗПЕКИ ХМАРНИХ РЕСУРСІВ

Марценюк Євгеній, Партика Андрій
Національний університет «Львівська політехніка»

Abstract: Метою даної роботи є розробка автоматизованого методу застосування конфігурацій публічних хмарних аккаунтів/підписок на AWS/GCP/Azure хостингу, та перервного сканування інфраструктури хмарних аккаунтів/підписок на невідповідність світовим стандартам безпеки (NIST 800-53, ISO 27001, HIPAA, PCIDSS)

Keywords: Хостинг, стандарти кібербезпеки, автоматизація, хмарні технології,

1. Вступ

На сьогодні більшість хмарних середовищ потребують впровадження засобів обліку, контролю зовнішнього периметру безпеки, контролю витрат та моніторингу з сторони спеціалістів по кібербезпеці. У більшості випадків процес застосування конфігурацій для створення хмарного середовища є однаковий та типовий в послідовності дій. Виходячи з цього можна автоматизувати цей процес та зекономити час та гроші на створення того що вже було створено не один раз.

Основним завданням даної роботи є створення сервісу для автоматичного застосування конфігурацій для створення хмарного середовища, його обліку у внутрішній системі обліку організації, облік доступів користувачі, контроль засобами моніторингу по логах за фінансами які витрачають сервіси хмарного середовища, конфігураціями зовнішнього периметра безпеки та постановка процесу контролю за критичними вразливостями та невідповідностями стандартам безпеки спеціалістами з кібербезпеки.

2. Дослідження поширених загроз безпеки інфраструктури хмарних середовищ

Основна проблема безпека в хмарному середовищі полягає в тому що відповідальність за безпеку провайдер розділяє з користувачем, більшість провайдерів надають доступи до своїх сервісів без включених контролів безпеки, що в свою чергу добре для процесу розробки сервісів, але створює вразливості для безпеки та витоків даних з хмарних середовищ.

Конфіденційність даних також стає все більш важливою для користувачів і державних установ. Згідно з Генеральним регламентом із захисту персональних даних (GDPR) і Законом про звітність і безпеку медичного страхування (HIPAA), організації мають збирати інформацію прозоро й упроваджувати політики, які допомагають запобігти викраденню або неналежному використанню даних. Недотримання цих вимог може призвести до значних збитків і підриву репутації організації. [1]

Базуючись на цьому принципі, можна виділити основні кроки які необхідно зробити власникам організації за для контролю безпеки:

- Визначити всіх постачальників хмарних середовищ, з якими працює організація, і ознайомитись з їхніми зобов'язаннями щодо безпеки та конфіденційності.
- Інвестувати в такі інструменти, які забезпечую захищений доступ до хмари, щоб слідкувати за всіма програмами й даними, які використовує організація. (Microsoft Azure Active Directory, AWS Identity, Google Authenticator, Okta)
- Розгорнути інструменти для керування захищеністю хмари, які вміють виявляти та виправляти помилки конфігурації (Prisma Cloud, Vanta).
- Провадити платформу захисту хмарної інфраструктури, щоб інтегрувати засоби безпеки в процес розробки. Регулярно встановлювати оновлення та патчі для програмного забезпечення та впровадити політики, щоб підтримувати пристрої працівників в актуальному стані. (end point protection)
- Впровадити процес навчання та оцінки обізнаності працівників принципам безпеки організації, щоб працівники були в курсі найновіших загроз і фішингових тактик.
- Впровадити стратегію захисту за моделлю «нульової довіри» та використати систему керування ідентичностями та доступом, для критичних вузлів інфраструктури.

3. Розроблення підходу «безперервного автоматизованого сканування конфігурацій» як елемента захисту хмарних середовищ

Незважаючи на наявність численних інструментів, більшості організацій важко ефективно контролювати доступ до своїх даних і застосовувати політику безпеки в хмарних середовищах, що постійно змінюються. Крім того, забезпечення відповідності, коли дані зберігаються в розподілених середовищах, створює значне навантаження на спеціалістів і без того обмежені групи безпеки. [2]

Сканування конфігурацій – це процес виявлення невідповідності налаштування по логам хмарного середовища (Audit logs, Flow logs) та співставлення конфігурації з рекомендованою стандартами кібербезпеки (NIST 800-53, HIPAA, PCIDSS, SOC, ISO)

Використовуючи постійну інтеграцію через audit та flow логування між хмарними середовищами та Prisma Cloud було досягнуто безперервного контролю за конфігураціями, зовнішнім периметром, витратами, управління змінами, авторизацією та зведення цих активів до відповідних стандартів безпеки. (див. Рисунок 1)

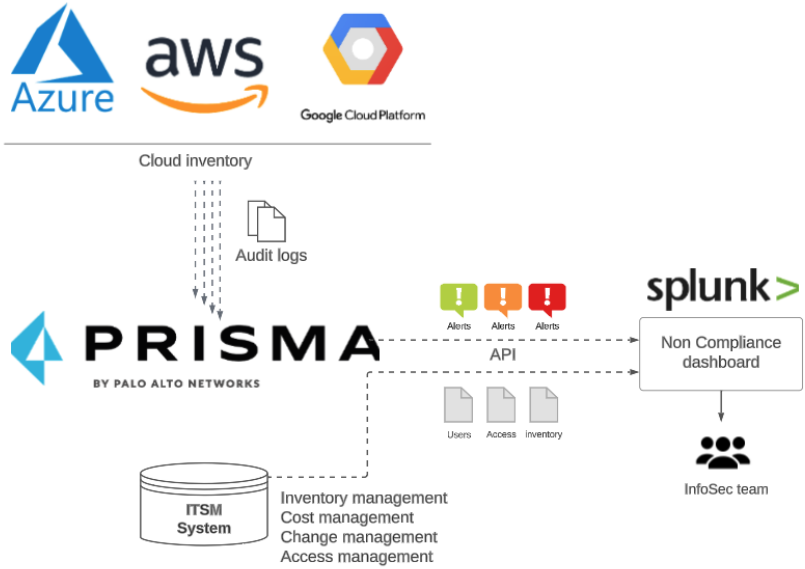


Рисунок 1 – Схема процесу сканування конфігурацій

Prisma Cloud™ —продукт PaloAlto Networks що дозволяє відстежувати конфігурації, співставляти їх з стандартами безпеки, проводити аналіз налаштування сервісів хмарних середовищ, ідентифікувати ризики та проводити автоматичні виправлення конфігурації згідно встановлених політик безпеки

ITSM System – система обліку активів організації. Містить відомості про активи, проекти, розподіл витрат, облікові зміни, облік системи авторизації та наданих доступів

Splunk – компанія, лідер ринку у SIEM (Security information and event management) - об'єднання двох термінів , що позначають область застосування

ПЗ: SIM (Security information management) – управління інформацією про безпеку, і SEM (Security event management) – управління подіями безпеки.

Технологія SIEM на базі Splunk забезпечує аналіз у реальному часі подій (тривог) безпеки, що виходять від мережевих пристроїв та додатків, і дозволяє реагувати на них до настання істотних збитків [4]

API — це набір визначень і протоколів для створення та інтеграції програмного забезпечення. Його іноді називають контрактом між постачальником інформації та користувачем інформації, який встановлює вміст, який вимагається від споживача (дзвінок), і вміст, який вимагає виробник (відповідь). [3]

Тестування відбувалось використовуючи інфраструктури хмарних середовищ Azure, AWS, GCP

4. Висновки

В даній роботі було запропоновано та спроектовано сервіс, який може бути використаний як механізм безперебійного та автоматизованого контролю за аккаунтами/підписками хмарних середовищ Azure (Microsoft), AWS (Amazon), GCP (Google)

Сервіс складається з наступних модулів:

- Контроль за конфігураціями – містить базові перевірки на відповідність стандартам безпеки
- Облік та аудит – містить компоненти які дозволяють проводити облік доступів користувачів, встановлювати обмеження по витратам, обліковувати зміни та встановлювати час існування активів що в свою чергу робить захист на актуальність того чи іншого активу
- Звітність та інформування – містить логіку інформування фахівців з кібербезпеки та дає змогу проводити аналітику того чи іншого хмарного середовища в одній точці

Література

1. Що таке безпека в хмарі https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cloud-security
2. Prisma: Cloud Governance & Compliance https://www.boll.ch/datasheets/ Prisma_Cloud_Governance_and_Compliance.pdf
3. What is a REST API? https://www.redhat.com/en/topics/api/what-is-a-rest-api
4. Security information and event management https://ru.wikipedia.org/wiki/SIEM#cite_note-:0-1

УДК 004.056

ОСОБЛИВОСТІ ЗАХИСТУ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ МЕРЕЖ ВІД АТАК НА АВТЕНТИФІКАЦІЮ

Махніцька Анастасія, Лагун Андрій
Львівський державний університет безпеки життєдіяльності

В сучасному суспільстві все частіше відбуваються атаки на мережі. Зловмисники можуть отримати доступ до конфіденційних даних та паролів користувача модифікувавши процеси автентифікації різними способами. В даній роботі наведено і проаналізовано можливі техніки які можуть бути використані для модифікації даних процесів та дії які варто впроваджувати для попередження таких атак.

Ключові слова: Зловмисники, автентифікація, програмне забезпечення, облікові дані.

In modern society, attacks on networks are occurring more and more often. Attackers can gain access to sensitive user data and passwords by modifying authentication processes in various ways. This work presents and analyzes possible techniques that can use to modify these processes and actions that should be implemented to prevent such attacks.

Keywords: Attackers, authentication, software, credentials.

В теперішньому інформаційному суспільстві надзвичайно важливою є проблема захисту мереж, адже сучасні кіберзлочинці стають все винахідливішими та агресивнішими. Створюються нові можливості для зламу мереж та доступу до особистих даних, адже зараз зростає кількість кібератак, суспільство все більше залежить від технологій, та відбується розширення інтернет речей. Тому захист мереж є критичним чинником, оскільки він впливає на безпеку, економіку та особисте життя кожної людини, а його відсутність може призвести до серйозних наслідків.

Загрози захисту мереж можуть включати в себе кібератаки (DDoS, віруси), соціальну інженерію (фішинг). Для захисту важливо використовувати багатошарові системи захисту, оновлювати програмне забезпечення, та використовувати сильні паролі. В цій роботі буде проведений аналіз деяких із загроз.

Також важливо відзначити можливість модифікації механізмів та процесів автентифікації. Адже зловмисники можуть отримати можливість втручатися в процеси автентифікації, зокрема зламувати локальний сервер автентифікації безпеки (LSASS) на операційних системах Windows, модулі автентифікації PAM на системах Unix, або авторизаційні плагіни на macOS. В результаті злочинці можуть отримати незаконний доступ до системи та вже існуючих облікових записів.

Зловмисник може змусити програму відкрити або дані потрібні для входу, або механізми автентифікації. Зламані облікові дані або доступ можна використати щоб оминути елементи контролю, розміщені на різних ресурсах системи всередині мережі та отримати можливість постійного доступу до віддалених систем та внутрішньо доступних сервісів, таких як VPN, пошта, доступ до мережі та віддалений робочий стіл.

Розглянемо детальніше конкретні техніки процесу модифікації автентифікації. Першою можна відмітити автентифікацію контролера домену (Domain Controller Authentication) – з цією технікою зловмисники можуть виправити процес автентифікації на контролері домену щоб обійти типові механізми автентифікації та забезпечити доступ до облікових записів.

Наприклад застосунок Skeleton Key використовують щоб встановити в процес автентифікації на контролері домену фальшиві дані та отримати незаконний доступ до облікового запису та особистих даних будь-якого користувача. Це програмне забезпечення вносить зміни до процесу автентифікації та надає злочинцю можливість входу з новими обліковими даними. Доступ до системи залишається до тих пір поки програмне забезпечення не буде видалено шляхом перезавантаження системи. Така атака створює загрозу для безпеки мережі та облікових даних.

Наступною технікою є бібліотеки динамічного компонування фільтрів паролів (password filter dynamic link libraries (DLLs)) – зловмисники можуть зареєструвати бібліотеки динамічного компонування (БДК) фільтрів паролів в процес автентифікації для отримання особистих даних користувача під час їх підтвердження. Ці бібліотеки можуть бути створені для збирання даних як і з окремих комп'ютерів так і з цілих доменів. За допомогою шкідливого програмного забезпечення Remsec злочинці отримують паролі які реєструються в системі у вигляді чистого тексту. Варто розуміти, що цю атаку важко виявити, адже вона відбувається на етапі входу в систему. Для запобігання таким атакам варто використовувати мультифакторну автентифікацію або ефективні механізми моніторингу та виявлення вторгнень.

Також нападники можуть використати атаки на підключені модулі автентифікації (Pluggable Authentication Modules) для доступу до облікових даних користувача або підключення небажаного доступу до акаунтів. PAM це модульна система конфігураційних файлів, бібліотек та виконавчих файлів які проводять автентифікацію для багатьох сервісів. Найбільш поширеним модулем є pam_unix.so, який повертає, підбирає та підтверджує облікові дані користувача. Зловмисники можуть користуватись додатком Skidmap, який вміє замінювати pam_unix.so файли на ураженій машині на свої зловмисні версії, які приймають конкретний запасний пароль для всіх користувачів. Щоб не наразитись на таку атаку варто обмежити доступ до системних файлів та моніторити зміни у системі PAM для виявлення незвичної активності, пов'язаної з автентифікацією. Також потрібно регулярно перевіряти цілісність файлів системи.

Наступною технікою, яку буде проаналізовано, є автентифікація мережевих девайсів (Network Device Authentication). Вона полягає в тому, що зловмисники можуть використовувати модифікований системний образ для жорсткого кодування пароля в операційній системі, таким чином обходячи власні механізми автентифікації для локальних облікових записів на мережевих пристроях. Використовуючи SYNful Knock – зловмисники можуть додати свої створені паролі «чорного входу» під час модифікації операційною системою ураженого мережевого пристрою. Таким чином, зловмисники отримують несанкціонований доступ та можливість впливу на мережевий трафік. Щоб отримати захист від такої атаки варто перевіряти цілісність та автентичність програмного забезпечення та регулярно оновлювати його.

Також часто використовують техніку зворотного кодування (Reversible Encryption) – для отримання паролів у відкритому тексті, коли в системі увімкнено властивість "AllowReversiblePasswordEncryption". Злочинці використовують цю функцію для доступу до облікових даних користувача та отримують пароль в зашифрованому форматі. Для розшифрування їм потрібні такі компоненти як: закодований пароль, рандомно згенероване значення, глобальний ключ місцевого органу безпеки та статичний ключ, який вбудований в механізм віддаленого доступу суп-автентифікації БДК. Щоб запобігти такій атаці варто відслідковувати, щоб властивість "AllowReversiblePasswordEncryption" була вимкнена.

Також слід відзначити можливість зловмисників впливати на механізми мультифакторної аутентифікації (МФА) та обходити їх. Це може включати вимкнення МФА або модифікацію функцій, що відповідають за автентифікацію в активному каталозі (Active Directory). Такі атаки можуть призвести до безперервного доступу до облікового запису та даних. Щоб не наразитись на таку небезпеку рекомендовано постійно відстежувати можливі порушення безпеки та регулярно оновлювати МФА.

Гібридна ідентичність (Hybrid Identity) – відноситься до ситуацій, коли користувачі використовують ідентифікатори локальних користувачів, а також ідентифікатори, пов'язані з хмарними послугами, для автентифікації та доступу до різних ресурсів та послуг. Зловмисники можуть намагатися використовувати цю гібридну ідентичність для своїх атак. Наприклад APT29 – редагує файли сервісного хоста для завантаження зловмисної БДК в процес автентифікації, дозволяючи постійний доступ до облікового запису. Щоб захиститись від цієї атаки важливо забезпечити надійний моніторинг та аудит безпеки. Також варто ретельно оновлювати та контролювати файли та процеси, пов’язані з автентифікацією.

Останньою технікою, на яку варто звернути увагу, є бібліотеки динамічного компонування мережевого провайдера (Network Provider DLL). Це компоненти, які дозволяють операційній системі Windows взаємодіяти з різними мережевими пристроями та протоколами. Натомість зловмисники

можуть намагатися використовувати ці бібліотеки для своїх атак, щоб захопити облікові дані користувачів під час процесу автентифікації. Під час входу в систему, Winlogon (модуль інтерактивного входу в систему) надсилає облікові дані на локальний mpnotify.exe процес. Потім mpnotify.exe ділиться обліковими даними в відкритому тексті із зареєстрованими менеджерами облікових даних під час сповіщення про подію входу. Зловмисник може налаштувати БДК на отримання даних від цього процесу. Якщо БДК встановлена менеджером облікових даних, то вона буде отримувати та зберігати облікові дані кожного разу, коли відбувається вхід в систему. Щоб запобігти такій атаці варто ретельно контролювати та перевіряти бібліотеки динамічного компонування мережевого провайдера, які використовуються в системі, та регулярно встановлювати оновлення безпеки.

На завершення можна зробити висновок, що для забезпечення високого рівня безпеки організації повинні постійно моніторити та аналізувати активність в мережі, шукати аномалії та незвичайну поведінку користувачів для того, щоб вчасно виявляти потенційні загрози та реагувати на них. Такий підхід допоможе зменшити ризик і вчасно виявляти можливі атаки на комп'ютерну систему.

Література

1. https://attack.mitre.org/techniques/T1556/
2. https://www.secureworks.com/research/skeleton-key-malware-analysis
3. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190154/The-ProjectSauron-APT_research_KL.pdf
4. https://opensource.apple.com/source/dovecot/dovecot-239/dovecot/doc/wiki/PasswordDatabase.PAM.txt
5. https://linux.die.net/man/8/pam_unix
6. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/managing_smart_cards/pluggable_authentication_modules

УДК 004.77

СУЧАСНІ ІНСТРУМЕНТИ ЗАХИСТУ МЕРЕЖІ

Мищак Юрій, Фединець Наталія
Львівський державний університет безпеки життєдіяльності, Львів

Анотація: У сучасному світі, де цифрові технології займають ключове місце у більшості аспектів життя та бізнесу, сучасні інструменти захисту мережі стали необхідністю. Вони допомагають захищати інформацію, забезпечувати надійність мереж та дотримуватися найвищих стандартів безпеки. Ці інструменти відіграють важливу роль у запобіганні кібератак, збереженні конфіденційності та цілісності даних, контролі доступу та автентифікації користувачів, виявленні та реагуванні на загрози, а також збереженні неперервності бізнесу.

Ключові слова: мережа, захист мережі, інструменти захисту мережі, інформаційна безпека.

Abstract: In today's world, where digital technologies occupy a key place in most aspects of life and business, modern network protection tools have become a necessity. They help protect information, ensure the reliability of networks and adhere to the highest security standards. These tools play an important role in preventing cyber attacks, maintaining data privacy and integrity, controlling access and user authentication, detecting and responding to threats, and maintaining business continuity.

Keywords: network, network protection, network protection tools, information security.

Сучасний захист мережі вимагає використання різноманітних інструментів та стратегій для захисту від різних видів загроз, включаючи хакерські атаки, віруси, шпигунський софт, DDoS-атаки та інші загрози. Для захисту мережі використовуються сучасні інструменти захисту мережі [2]:

1. Брандмауери (Firewalls): Брандмауери – це пристрої, програми або сервіси, які фільтрують трафік, що надходить у мережу та виходить з неї. Вони визначають, який трафік допускається та який блокується на основі заданих правил.

2. Антивірусне програмне забезпечення: Антивірусні програми виявляють та блокують шкідливий код, віруси, троянські коні та інші загрози для комп'ютерів та мережі.

3. Системи виявлення та запобігання вторгненням (Intrusion Detection and Prevention Systems, IDS/IPS): Ці системи виявляють аномальну активність в мережі і виконують дії для зупинки або блокування потенційних вторгнень.

4. VPN (Virtual Private Network): VPN дозволяє створити зашифроване з'єднання між вузлами мережі, що забезпечує конфіденційність та безпеку передачі даних через відкриті мережі, такі як Інтернет.

5. Системи керування ідентифікацією та доступом (Identity and Access Management, IAM): IAM системи дозволяють адміністраторам керувати правами доступу користувачів до різних ресурсів мережі та додатків.

6. Шифрування: Шифрування даних забезпечує конфіденційність інформації під час передачі та зберігання даних.

7. Мережева безпека на рівні пристроїв: Встановлення оновлень, паролів та налаштування захисту на рівні пристроїв, таких як маршрутизатори та комп'ютери, допомагає уникнути вразливостей та атак.

8. Системи моніторингу та аналізу журналів: Ці системи відстежують активність мережі та реагують на підозрілі події.

9. Антивирусні шлюзи та шлюзи контент-фільтрації: Вони фільтрують трафік, який виходить із мережі та надходить до неї, для блокування шкідливого вмісту.

10. Швидке відновлення та резервне копіювання даних: Забезпечення резервних копій та можливості швидкого відновлення даних допомагає захистити важливу інформацію від втрати.

11. Системи моніторингу та аналізу кіберзагроз: Вони використовуються для виявлення та аналізу загроз у реальному часі, що допомагає реагувати на потенційні атаки.

12. Безпека IoT (Internet of Things): Завдяки росту IoT пристроїв, важливо забезпечити їх безпеку та інтегрувати їх у мережу з належним захистом.

Ці інструменти та технології часто комбінуються для створення комплексної стратегії захисту мережі, оскільки загрози постійно змінюються і стають більш складними. При цьому важливо також використовувати практики та навчати персонал щодо кібербезпеки для мінімізації ризику інцидентів.

Одним з сучасних існтрументів захисту мережі є програма XSpider. XSpider – це графічна система проектування, яка дає змогу промальовувати низьковольтні мережі, оснащені обладнанням для захисту електричних кіл виробництва компанії Eaton [1]. Вона обчислює падіння напруги, розподіл навантаження та струми короткого замикання для радіальної, а також сітчастої мережі та здійснює подальшу перевірку придатності кабелів та захисного обладнання. Програмне забезпечення надає проектувальникам та інженерам інструмент планування, який забезпечує дотримання сучасних стандартів та урахування рівнів ризику утворення дугового розряду. Усі розрахунки проведено згідно зі стандартами IEC.

Основні можливості XSpider включають:

1. Вилучення тексту, зображень, посилань та інших даних з вебсайтів.

2. Навігація по різних сторінках сайту та взаємодія з формами.
3. Збереження даних в різних форматах, таких як CSV, Excel, бази даних тощо.
4. Розкладання завдань на автоматизовані процедури.
5. Можливість створювати складні логічні конструкції для обробки даних.
6. Планування та виконання завдань на регулярній основі.
7. Підтримка інструментів для аналізу та візуалізації даних.

XSpider використовується в різних галузях, таких як бізнес-аналітика, фінансові послуги, маркетинг, наукові дослідження та інші сфери, де важливо автоматизувати процеси збору та обробки даних з Інтернету. Однак важливо враховувати, що використання XSpider повинно дотримуватися законів та правил використання даних та бути етичним.

Застосування сучасних інструментів захисту мережі є важливою частиною стратегії інформаційної безпеки та вимагає постійного оновлення та адаптації до зростаючих кіберзагроз. Забезпечення надійної та ефективної мережевої безпеки стає критично важливим завданням у світі, де обмін інформацією та зберігання даних зростають в значущості, і де безпека є пріоритетом для організацій і індивідів.

Література

1. Eaton. URL: https://www.eaton.com/ua/uk-ua/catalog/low-voltage-power-distribution-controls-systems/ xspider.htmlFotocvetov: огляд. URL: fotocvetov-https://fotocvetov.com/allinnews/spravka&co&uu/posts/skaner/uk/bezopasnost-skaner-vrazlivostej-xspider-7/

УДК 004.056.5

КРИПТОЛОГІЯ: СУЧАСНІ ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ

Моравський Владислав, Ткачук Ростислав, Колос Надія
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. Історія криптології налічує більше двох тисячоліть. Вона розпочинає свій розвиток від використання простих шифрів в стародавньому світі, та переживає значні метаморфози впродовж подальшого становлення. Приймає різноманітні виклики та вирішує складні задачі пов'язані із шифруванням та передачею інформації, обміном ключами та їхнім керуванням. Використовує найсучасніші квантові технології для вирішення поставлених задач – захисту інформації в сучасному цифровому суспільстві.
Ключові слова: криптологія, шифрування, історія криптології, інформаційна безпека.

Abstract. The history of cryptology dates back more than two millennia. It begins its development with the use of simple ciphers in the ancient world, and undergoes significant metamorphoses during its further development. It accepts various challenges and solves complex tasks related to encryption and information transmission, key exchange and their management. It uses the most modern quantum technologies to solve the tasks – information protection in the modern digital society.
Keywords: cryptology, encryption, history of cryptology, information security.

Криптологія — розділ науки, що вивчає методи шифрування і дешифрування інформації. Вона поділяється на два розділи: криптографію та криптоаналіз. Це науки про математичні методи, відповідно, забеспечення та порушення конфіденційності, цілісності та автентичності інформації.

Перші шифри з'явились ще за часів античності більше 2000 років тому, наприклад:

– Атбаш, використовували на ближньому сході. Основна ідея цього шифру в тому, що кожна літера тексту замінюється на літеру, яка розташована в зворотному алфавітному порядку. Наприклад, "A" замінюється на "Z", "B" на "Y" і так далі.

– Скитала, використовували в Греції. Основна ідея шифру Скитала полягає в тому, щоб намотати шкіряну стрічку на циліндр. Перпендикулярно стрічці писалось повідомлення, потім стрічка розмотувалась і передавалась одержувачу. В цьому випадку ключом є діаметр циліндра намотування.

– Шифр Цезаря, він використовує зсув символів в алфавіті на певну кількість позицій. Недолік цього шифру в тому, що існує мала кількість варіантів зсуву, які досить легко порахувати [1].

З часом з'явився більш складний шифр, в якому кожному символу з алфавіту підставлявся інший випадковий символ з цього ж алфавіту, буду-

ючи таким чином таблицю для шифрування. Основним недоліком такого підходу була складність у запам'ятовуванні таблиці. Рішенням цієї проблеми, була відмова від випадкової підстановки і побудова простих алгоритмів таблиці шифрування.

В 9 ст. арабський вчений Абу Юсуф Якуб ібн Ісхак ібн Саббах аль-Кінді написав книгу "Трактат про дешифрування криптографічних повідомлень", в якому, вперше був описаний метод частотного криптоаналізу для злому шифру, який ґрунтується на частоті появи символів в тексті. З появою частотного криптоаналізу шифри складені за попередніми алгоритмами частково втратили свою надійність. Протягом наступних століть були реалізовані різні ідеї і методи ускладнення шифру: додавались шуми, мінявся порядок слів, тощо. Всі ці методи робили процес шифрування більш складним, довгим, але в кінцевому результаті, все зводилося лише до ускладнення злому шифру.

Новим кроком в шифруванні повідомлень стали поліалфавітні шифри, яскравим представником яких був шифр Віженера. Основна ідея цього шифру полягає в тому, щоб використовувати ключ, який є словом або фразою, для зміни зсуву символів в алфавіті під час шифрування [1]. Процес шифрування використовує ключове слово або фразу, як вихідну точку. Кожна буква ключа відповідає певному зсуву символів. Таким чином повідомлення шифрується шляхом зсуву кожної букви на відповідну кількість позицій в алфавіті, залежно від конкретної букви ключа. Дешифрування повідомлення виконується за допомогою того ж самого ключа, але в зворотному напрямку. Шифр Віженера був більш безпечним, порівняно з іншими шифрами того часу, оскільки він виявився стійкішим до частотного криптоаналізу. Протягом 300 років цей шифр вважався незламним. Він не був дуже популярний адже для його використання треба було витрачати по декілька годин на шифрування та дешифрування.

Виникла ситуація, в якій надійне шифрування вимагало багато часу і ресурсів, а більш прості шифри швидко зламувались. Ситуація ще ускладнилась, коли в 1863 році Фрідріхом Вільгельмом Казіскі була опублікована книга "Тайнопис і мистецтво дешифрування", в якій був описаний алгоритм злому шифру Віженера. Цю кризу інформаційної безпеки врятувала поява перших роторних машин шифрування. Вони дозволили швидко і просто використовувати складні шифри. Така ситуація сприяла значному росту об'ємів зашифрованої інформації, хоча, по суті не збільшувала надійність самого шифрування.

Згодом, було проведено фундаментальне дослідження шифру Віженера, за результатами якого був запропонований одноразовий ключ — набір випадкових символів, який був рівний за довжиною шифрованому тексту. Такий підхід, з однієї сторони, забезпечував абсолютну криптографічну стійкість, з іншої, мав невиправдано високу вартість та незручність у використанні [1, 3].

Під час Першої світової війни, криптологія і зокрема криптоаналіз, стає одним з інструментів ведення війни.

Перемога німців над переважаючими силами російської армії в битві під Танненбергом і розшифрування повідомлення Цимермана (яке сприяло вступу до війни США), а також злам німецького шифру у червні 1918 року французьким криптоаналітиком Жаном Жоржем Пенвеном (що дав змогу дізнатись напрямок німецького наступу), - це одні з яскравих прикладів впливу криптології [2].

Ще більший вплив криптологія мала на перебіг Другої світової війни. Уже перед початком воєнних дій, провідні держави використовували електромеханічні шифрувальні пристрої, що робило завдання злому шифру досить нетривіальною задачею [1].

Під час війни союзникам вдалося двічі зламати німецькі шифри. Для злому шифрів була, вперше, реалізована ідея використати криптографічні машини не тільки для шифрування, а й для злому.

Колосальний вплив на криптографію мали ЕОМ. Вони призвели до того, що замість шифрування тексту почали шифрувати двійковий код. Разом з тим, появились більш прогресивні генератори випадкових чисел, тому розшифрувати інформацію без знання ключа стало практично не можливим. Проте виникла нова проблема – передача самого ключа, оскільки відправляти ключ по відкритим каналам – небезпечно. Рішенням цієї проблеми став асиметричний ключ. Логіка цього методу полягає в створенні 2-х ключів, особистого і публічного. Шифр побудований таким чином що повідомлення зашифроване публічним ключом можливо розшифрувати тільки приватним ключом такий механізм працює з математичними перетвореннями які легко провести в одному напрямку і дуже важко в іншому. Цей підхід, на сьогодні, вважається досить надійним [2, 3].

Але розвиток цифрових технологій невпинно прогресує. Набувають широкого використання квантові технології, які в рази збільшують швидкість проведення обчислювальних операцій, і можуть перетворити сучасні найнадійніші криптографічні алгоритми в ненадійні методи шифрування [4].

З іншого боку поступово починає розвиватись і квантова криптологія. На сьогоднішній день вже існують принципи і методи шифрування за якими інформацію неможливо перехопити і розшифрувати залишаючись непоміченим. Проте є і деякі суттєві недоліки, які пов’язані з передачею даних (квантів) по бездротовій мережі, крім того вони є дуже нестабільні що наразі обмежує дальність зв'язку до 100 км.

Також розвиток у галузі штучного інтелекту вплинув на досягнення у криптології. Методи штучного інтелекту (ШІ) можна застосовувати до криптографічних проблем різними способами. Мета полягає в тому, щоб більш детально зрозуміти потенційні атаки та гарантії безпеки криптографічних методів і реалізацій. ШІ можна використовувати для вдосконалення або автоматизації методів атак, а також для створення доведення безпеки

або виявлення помилок у доведеннях безпеки. І навпаки, криптографічні методи також можна використовувати для зменшення проблем у застосуванні методів штучного інтелекту, таких як методи машинного навчання та логічного виведення, що зберігають конфіденційність.

Нейронна криптографія [5] — це розділ криптографії, присвячений аналізу застосування стохастичних алгоритмів, особливо алгоритмів штучних нейронних мереж, для використання в шифруванні та криптоаналізі. Через високу практичну значимість таких моделей ШІ як штучні нейронні мережі для оцінки безпеки криптографічних реалізацій, міжнародні відомства з інформаційної безпеки активно стежать за прогресом у сфері аналізу побічних каналів [6] за допомогою методів ШІ, а також роблять внесок у дослідження в цій галузі.

Як видно з історії між криптографами і криптоаналітиками існує жорстке протистояння в якому на даний момент беруть верх криптографи, забезпечуючи захист інформації від несанкціонованого доступу.

Література

1. Гребенніков В. Історія криптології і секретного зв'язку / Гребенніков В. – К.: Каравела, 2012. – 327 с.

2. Електронний ресурс https://www.wikiwand.com/uk/ Криптографія_Першої_світової_ війни.

3. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с. – Доступ: http://ela.kpi.ua/handle/123456789/23896

4. Криптографічні та стенографічні засоби захисту інформації. Полотай О.І., Овчиннікова К., Лагун А.Е. Зб. тез доп. IV Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології". (м. Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 146–148.

5. Neural Network-Based Cryptography: A Primary Study on the Performances and Techniques/ Jia-Lin Foo, Kok-Why Ng, Palanichamy Naveen/ Proceedings of the International Conference on Computer, Information Technology and Intelligent Computing (CITIC 2022). – 2022. – p. 68-78.

6. Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning/Gohr, A. /Advances in Cryptology – CRYPTO 2019. Lecture Notes in Computer Science, vol 11693, – p. 150-179.

УДК 004.056.5

ВІД АВТОМАТИЗАЦІЇ ДО ЗАГРОЗ: РОЗУМІННЯ ДИНАМІКИ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Навитка Марія, Венгрин Василина
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. В роботі розглянуто вплив штучного інтелекту (ШІ) на кібербезпеку, на перевагах та недоліках використання ШІ в цій області. Визначено, що ШІ дозволяє обробляти великі обсяги даних та автоматизувати виявлення кіберзагроз, проте застерігає від можливості використання ШІ зловмисниками для створення ефективних кібератак. Рекомендовано багаторівневий підхід до кібербезпеки та поставлено акцент на важливості етичного використання технологій ШІ.

Ключові слова: штучний інтелект, кібербезпека, автоматизація, кіберзагрози, моніторинг безпеки.

Abstract. The study examines the influence of artificial intelligence (AI) on cybersecurity, detailing the benefits and drawbacks of its application in this domain. It is noted that AI facilitates the processing of extensive data and automates the identification of cyber threats, while also warning about the possibility of malicious actors exploiting AI for crafting sophisticated cyber attacks. A multilayered approach to cybersecurity is advised, underscoring the significance of ethically deploying AI technologies.

Keywords: artificial intelligence, cybersecurity, automation, cyber threats, security monitoring.

У контексті невпинно зростаючих кіберзагроз та стрімкої еволюції штучного інтелекту, важливо розглянути, як саме ці технології взаємодіють та формують майбутнє кібербезпеки. В цій динамічній атмосфері, де інновації стають відповіддю на загрози, розгортається новий погляд на стратегії захисту та використання ШІ для досягнення вищого рівня безпеки в цифровому просторі. Важлива подія – поява відкритих інструментів штучного інтелекту, таких як ChatGPT та Bard.

Перевага ШІ в кібербезпеці. Здатність обробляти величезні обсяги даних. Компанії можуть аналізувати величезні обсяги даних з неймовірною точністю та ефективністю завдяки штучному інтелекту в кібербезпеці. Штучний інтелект автоматизує створення алгоритмів машинного навчання, які можуть ідентифікувати різноманітні проблеми кібербезпеки, включаючи спам, веб-сайти з загрозами, програми сторонніх розробників і спільні дані.

Недоліки. Більше даних означає більше проблем. Підприємства, які використовують ШІ для обробки даних, зараз роблять це з безпрецедентною швидкістю. Але передача нашої конфіденційної інформації зовнішнім компаніям ризикує порушити нашу конфіденційність.

Хакери потенційно можуть отримати прибуток від розробки штучного інтелекту, оскільки це полегшить їм здійснення дуже ефективних і масштабних кібератак. Слабкі місця мережі даних або комп’ютерної системи також можна належним чином дослідити та використовувати за допомогою ШІ.

Наші секретні та конфіденційні дані можуть опинитися під загрозою через гаджети на основі ШІ, як-от біометричні системи. Конфіденційність як окремих осіб, так і компаній може бути порушена здатністю цих гаджетів надсилати наші дані ненадійним стороннім постачальникам.

За допомогою передових мовних модулів, як ChatGPT, кіберзлочинцям стало простіше створювати фішингові листи та атаки. Ці інструменти миттєво генерують розмовний текст, дозволяючи зловмисникам переконливо імітувати стиль спілкування довірених осіб чи організацій та збільшувати ефективність своїх атак. У майбутньому кіберзлочинці, ймовірно, комбінуватимуть ці мовні моделі з генерованими ШІ зображеннями, аудіо- та відеокліпами, щоб обманювати користувачів і змушувати їх розкривати конфіденційну інформацію та надавати доступ до комп'ютерних систем.

Використання штучного інтелекту, включаючи ChatGPT, дозволяє кіберзлочинцям автоматизувати та масштабувати свої атаки, роблячи їх ефективнішими. Навіть новачки можуть використовувати ці інструменти для створення шкідливого коду та усунення несправностей у існуючих вірусах, щоб зробити їх більш небезпечними. Незважаючи на деякі заходи захисту, ChatGPT можна обійти і використати для оптимізації розробки шкідливого програмного забезпечення та автоматизації атак.

Використання штучного інтелекту в кібербезпеці може допомогти організаціям зміцнити захист та зняти навантаження зі спеціалістів. Інструменти на базі ШІ дозволяють автоматизувати рутинні завдання у сфері безпеки, звільняючи час експертів для найважливіших завдань. ШІ також може використовуватися для моніторингу та аналізу подій безпеки, виявлення аномалій та прискорення виявлення загроз. Алгоритми машинного навчання виявляють шкідливу активність, дозволяючи фахівцям зосередитися на розслідуванні та усуненні загроз.

Насамперед організації повинні застосовувати багаторівневий підхід до безпеки, щоб зміцнити свою кіберстійкість, оскільки потужні технології ШІ продовжують ставати все більш поширеними. Їм слід запровадити передові методи навчання з питань безпеки, щоб допомогти співробітникам зрозуміти складність сучасних загроз. Також організаціям рекомендується застосовувати штучний інтелект у технологіях безпеки для покращення моніторингу, виявлення та реагування на загрози. Ці інноваційні технології будуть корисними та допоможуть командам з безпеки більш ефективно протидіяти загрозам.

В останні роки штучний інтелект став важливою частиною обладнання для підтримки роботи команд захисту інформації людини. Оскільки люди більше не в змозі масштабуватись, щоб ефективно захистити динамічну поверхню бізнес-атак, штучний інтелект пропонує критичний аналіз і виявлення загроз, які можуть використовувати експерти з кібербезпеки для зниження ризику злому та посилення безпеки.

Штучний інтелект у сфері безпеки може визначати пріоритети ризиків, негайно ідентифікувати будь-яке зловмисне програмне забезпечення в мережі, направляти реагування на інциденти та виявляти атаки до їх виникнення.

Штучний інтелект дозволяє командам із кібербезпеки створювати міцні альянси між людиною та машиною, які покращують наше розуміння, покращують наше життя та просувають кібербезпеку.

Використання штучного інтелекту у кібербезпеці відкриває нові можливості та виклики. Важливо усвідомлювати, що це не тільки потужний інструмент для виявлення та запобігання загроз, але й потенційний ризик для приватності та безпеки даних. Розуміння цих аспектів та активна реакція на них дозволять ефективно дослідити взаємозв'язки між автоматизацією та загрозами, які може призвести використання штучного інтелекту в кібербезпеці. З одного боку, автоматизація та обробка великих обсягів даних ШІ дозволяють виявляти та протидіяти кіберзагрозам з неймовірною точністю та ефективністю. З іншого боку, бачимо ризики, пов'язані з можливістю зловмисників використовувати ШІ для створення вдосконалених кібератак.

Отже, важливою є рекомендація впровадження багаторівневого підходу до кібербезпеки, що включає в себе не лише ШІ, але й інші методи та техніки. Також, особливу увагу приділити етичним аспектам використання технологій ШІ, щоб уникнути можливості порушення приватності та недозволеного використання даних.

Постійне вдосконалення стратегій кібербезпеки в умовах динамічного цифрового середовища та активного впровадження інновацій забезпечить стійкий захист від сучасних кіберзагроз.

Література

1. Abeshu A, Chilamkurti N, 2018. Deep learning: the frontier for distributed attack detection in fog–to–things computing. IEEE Commun Mag, 56(2):169–175. https://doi.org/10.1109/MCOM.2018.1700332

2. George Baryannis, Sahar Validi, Samir Dani & Grigoris Antoniou (2019) Supply chain risk management and artificial intelligence: state of the art and future research directions, International Journal of Production Research, 57:7, 2179-2202, https://doi.org/10.1080/00207543.2018.1530476

3. Jin, D.; Jin, Z.; Zhou, J.T.; Szolovits, P. Is Bert really robust? A strong baseline for natural language attack on text classification and entailment. Proc. AAAI Conf. Artif. Intell. 2020, 34, 8018–8025. [Google Scholar]

4. Mhlanga, David, Open AI in Education, the Responsible and Ethical Use of ChatGPT Towards Lifelong Learning (February 11, 2023). Available at SSRN: https://ssrn.com/abstract=4354422 or http://dx.doi.org/10.2139/ssrn.4354422

УДК 004.056.5

ІНТЕЛЕКТУАЛЬНА БЕЗПЕКА В МОДНІЙ ІНДУСТРІЇ

Навитка Марія, Водніцька Олена, Яхура Анастасія
Львівський державний університет безпеки життєдіяльності,
Лапаївський ліцей імені Героя України Георгія Кірпи
Зимноводівської ОТГ

Анотація. Розглянуто інтеграцію штучного інтелекту (ШІ) в індустрію моди для автентифікації предметів розкоші та боротьби зі зростаючим ринком підробок. У тексті детально описуються функції та кейси використання ШІ відомими брендами, підкреслюються екологічні та етичні переваги цих технологій. Крім того, висвітлено їхні потенційні перспективи для вдосконалення процесів автентифікації та пом'якшення негативного впливу на довкілля.

Ключові слова: автентифікація, мода, брендові товари, екологічні та етичні проблеми, сегментація зображення.

Abstract. The integration of artificial intelligence (AI) into the fashion industry to authenticate luxury goods and combat the growing counterfeiting market is considered. The text describes in detail the functions and use cases of AI by well-known brands, emphasizing the environmental and ethical advantages of these technologies. Moreover, it highlights their potential prospects for improving authentication processes and mitigating negative environmental impact.

Keywords: authentication, fashion, luxury goods, environmental and ethical issues, image segmentation.

В сучасному світі індустрія моди не лише ставить перед нами безмежний вибір естетичних вражень, але й видається складною мережею проблем, які виникають у зв'язку зі зростанням чорного ринку модних підробок. Пробуючи забезпечити якість та автентичність своїх продуктів, бренди елітних товарів активно впроваджують технології штучного інтелекту. Цей вступ докладає спроби вирішити екологічні та етичні проблеми, пов'язані з модою, за допомогою передових засобів автентифікації та боротьби зі злочинністю в цій галузі.

Виробництво модних підробок несе екологічні та етичні проблеми. Модні бренди тепер покладаються на технологію Al для виявлення підробок і збереження ідентичності бренду. Розкішні бренди та компанії використовують технологію ШІ для забезпечення себе системами аутентифікації на основі даних, щоб перехитрити фальшивомонетників, які представляють глобальний чорний ринок вартістю 1,9 трильйона доларів, що становить близько 3,3% світової торгівлі. Приклад цієї технології можна побачити в недавньому запуску LVMH-бренду Patou системи перевірки штучного інтелекту під назвою Authentique Verify, зробленої у співпраці з технологічним партнером Одрі.

Завантажуючи знімок, зроблений за допомогою камери телефону та спеціального додатка, система обробляє мікроскопічні властивості автентичних продуктів, подібно до відбитків пальців, роблячи їх неможливими для повторного відтворення. Хоча докази підтверджують ефективність цієї технології, експерти припускають, що найкращі результати виникають у поєднанні ШІ з експертними людськими автентифікаторами.

Передові методи виробників чорного ринку для створення контрафактної продукції, таких як лазерне різання та 3D-друк, виробляють майже непомічені копії, які навіть кидають виклик оригінальним творцям. Ці системи на базі штучного інтелекту створені для охоплення цифрової енциклопедії властивостей як підроблених, так і автентичних статей, використання інформації для виявлення тонких невідповідностей тканини, зшивання або металів, які допомагають відрізнити справжні предмети від підробок. Він також може вивчати цифрові дані, такі як серійні номери продуктів, замовлення на купівлю та платіжну інформацію, щоб відповідати підписам оригінальних продуктів з підробками та виявлення будь-яких розбіжностей. Потенціал ШІ для боротьби фальшивомонетниками проявляється через історії успіху, такі як Burberry, який використовує технологію розпізнавання зображень для визначення автентичності продукту на основі найдрібніших деталей у ткацтві та текстурі з точністю 98%.

Подібним чином такі компанії, як Jimmy Choo та Deloitte, Dupe Killers, використовують технологію, що працює на ШІ, для пошуку порушень дизайну та захисту репутації свого бренду. Entrupy - ще одна компанія, що розробляє інструменти машинного навчання, щоб допомогти покупцям перевірити автентичність продукту. Їх камера зі штучним інтелектом збільшує тканини, щоб розкрити невидимі функції, перевіряючи сотні тисячі особливих характеристик продукту, таких як колір, зшивання та шкіряні візерунки. Спочатку вони розробили антиконтрафактні алгоритми на основі величезних баз даних інформації про топові люксові бренди, а потім за допомогою сканера здатні миттєво виявити імітаційні дизайнерські сумки, аналізуючи мікроскопічні знімки деталей матеріалу, майстерності, серійних номерів та зносу.

Існує три типи прикладних технологій, які доступні для виявлення підроблених предметів моди. Першою такою технологією є класифікація зображень, яка використовується для автоматичної класифікації різних предметів одягу. Класифікація зображень знаходить застосування в автоматичному сортуванні одягу, рекомендації вмісту та класифікації атрибутів. Його можна додатково розділити на класифікацію, засновану на стилях одягу та класифікації на основі атрибутів одягу, перша зосереджується на визначенні таких категорій, як взуття, топи та штани. По-друге, це сегментація зображення, яка дозволяє розрізняти піксельний рівень одягу, штанів та різних аксесуарів у зображенні моди. По-третє, це визначення координа-

тних точок одягу в зображенні. Його можна класифікувати на виявлення цілей та виявлення ключових точок. Обидва типи включають визначення координатних точок одягу в зображенні, що є цінним для пошуку та розпізнавання одягу.

Шкідливий вплив підробок виходить за межі клієнтів і брендів. Навколишнє середовище та працівники, які беруть участь у виробництві шахрайських товарів, також негативно впливають. Контрафактна продукція зазвичай виготовляється на нерегульованих заводах в поганих і небезпечних умовах. Виявлення шахрайства на базі ШІ стало можливим, особливо в індустрії моди, де ручне виявлення було 6 недоцільним через величезну кількість продуктів. В даний час процес виявлення контрафакту є дорогим і трудомістким, в той час як генеративні змагальні мережі і передача навчання обіцяють прискорити процес та зменшення витрат у майбутньому. Крім того, модні бренди можуть платити платежі постачальникам, що надають цю послугу, щоб захистити себе від значних втрат доходів.

У світі моди й виробництва брендових товарів використання штучного інтелекту в процесі автентифікації визначається не лише стратегічною необхідністю, але й ключовим інструментом для подолання екологічних, етичних та економічних проблем. ШІ відкриває шлях до новаторських рішень у сфері боротьби з чорним ринком та виробництвом підробок. Бренди, такі як LVMH Patou та Burberry, вже успішно впроваджують технології, які забезпечують високий рівень автентифікації, використовуючи класифікацію, сегментацію та аналіз даних. Інновації у сфері автентифікації за допомогою ШІ визначають та формують майбутнє індустрії, що дозволяє вдосконалити весь процес, забезпечуючи якісну захист брендів та зацікавлених сторін у світі моди.

Література

1. https://hypebeast.com/2019/9/lvmh-backs-entrupy-handbag-authentication-tech
2. https://ww.fashionnetwork.com/news/Entrupy-takes-its-ai-based-counterfeit-spotting-technology-to-asia-sets-up-operations-in-japan,943594.html
3. https://shoparticleconsignment.com/blogs/authenticity/entrupy-authentication-software
4. https://www.the-hosta.com/pages/what-is-entrupy-luxury-authentication
5. https://ww.fashionnetwork.com/news/Entrupy-takes-its-ai-based-counterfeit-spotting-technology-to-asia-sets-up-operations-in-japan,943594.html

УДК 004.05

ОСОБЛИВОСТІ КІБЕРБЕЗПЕКИ ДЛЯ СУЧАСНИХ НАУКОВИХ ДОСЛІДЖЕНЬ

Навитка Марія, Навитка Святослав
Львівський державний університет безпеки життєдіяльності,

Анотація. У статті розглядається поняття кібербезпеки та роль цифрових технологій у виявленні та захисті наукових досліджень від кібератак. Визначено, що цифрові технології відіграють вирішальну роль у забезпеченні безпеки наукового середовища, зокрема за допомогою механізмів виявлення, адаптивного захисту та спільних зусиль. Надано рекомендації, які включають використання передових технологій кібербезпеки, навчання персоналу з питань безпеки та розробку ефективних стратегій реагування на кіберзагрози, що, в свою чергу, забезпечить сталість та цілісність наукових досліджень.

Ключові слова: цифрові технології, наукові дослідження, адаптивні заходи захисту, динамічні системи виявлення інцидентів, кіберзагрози, інформаційна безпека.

Abstract. The article discusses the concept of cybersecurity and the role of digital technologies in detecting and protecting scientific research from cyberattacks. It is determined that digital technologies play a crucial role in ensuring the security of the scientific environment, in particular through detection mechanisms, adaptive protection and joint efforts. Recommendations are provided, including the use of advanced cybersecurity technologies, security training for personnel and the development of effective strategies for responding to cyber threats, which, in turn, will ensure the sustainability and integrity of scientific research.

Keywords: digital technologies, scientific research, adaptive security measures, dynamic incident detection systems, cyber threats, information security

У сучасному інформаційному суспільстві, де обсяг наукових досліджень швидко зростає, використання цифрових технологій стає невід'ємною частиною наукового процесу. За всіма позитивними здобутками, які ці технології приносять, стоїть велика відповідальність щодо забезпечення безпеки та недоторканості наукових даних. Задача виявлення та захисту від кібератак стає критичною для забезпечення інтегрітету (непорушності, цілісності) та безпеки наукових досліджень у віртуальному просторі.

Цифрові технології в значній мірі змінили підхід до виконання наукових досліджень. Вони не лише відкривають безмежні можливості для збору, обробки та аналізу даних у наукових дослідженнях, але й стають мішенню для кіберзагроз, які спрямовані на вразливості в цифрових інфраструктурах. Ця напруга між інноваційністю та безпекою визначає новий контекст для розуміння ролі цифрових технологій у науковому середовищі.

Досягнення цих цілей вимагає постійного вдосконалення та апгрейду цифрових технологій, розробки нових алгоритмів захисту та впровадження сучасних стандартів безпеки. Зрозуміння ролі цифрових технологій у виявленні та захисті наукових досліджень не лише визначає майбутнє наукового світу, але й формує основи для сталого інноваційного розвитку, де цифрова безпека є неодмінною передумовою для високоякісного наукового виробництва.

У цьому контексті, важливо проаналізувати, як цифрові технології впливають на виявлення потенційних загроз для наукових досліджень та які заходи захисту можна впровадити для збереження конфіденційності та недоторканості цих досліджень у віртуальному просторі. Подальше розглядання цих питань дозволить розкрити нові перспективи для розвитку та забезпечення стійкості наукового середовища в умовах постійних технологічних викликів та кібернебезпеки.

Розвиток сучасних цифрових технологій неминуче породжує нові виклики у сфері кібербезпеки, особливо коли йдеться про захист наукових досліджень. У зв'язку з постійним зростанням загроз і вдосконаленням методів кібератак, важливо створити адаптивні заходи захисту, які забезпечать невідкладну реакцію на швидкозмінні сценарії атак. Розглянемо деякі з них.

1. Однією з основних складових адаптивного захисту є використання динамічних систем виявлення інцидентів. Ці системи використовують алгоритми машинного навчання та штучного інтелекту для аналізу великого обсягу даних і виявлення непередбачуваних патернів, характерних для нових кіберзагроз.

2. Розробка автоматизованих реакційних механізмів є необхідністю для оперативної відповіді на кібератаки. Ці механізми можуть включати в себе автоматичні системи блокування доступу, ізоляції заражених систем або автоматичного відновлення даних з резервних копій.

3. Використання розширених аналітичних інструментів, які базуються на штучному інтелекті, дозволяє не лише виявляти загрози, але й робити прогнози та адаптуватися до нових видів кібератак. Ці інструменти можуть вивчати поведінку зловмисників і виявляти їхні тенденції, що є важливим для вдосконалення заходів захисту.

4. Використання систем штучного інтелекту, спроможних самостійно аналізувати та класифікувати потенційні загрози, є важливим аспектом адаптивного захисту. Ці системи можуть оперативно реагувати на нові види загроз та вчитися на основі нових даних, що дозволяє швидко адаптувати стратегії захисту.

5. Суттєвим елементом адаптивного захисту є розробка контингентних планів та сценаріїв реагування на кібератаки. Вони враховують різні варіанти атак та забезпечують деталізовані кроки для відновлення після інциденту.

6. Адаптивний захист передбачає постійне навчання та співпрацю між науковими групами. Організації повинні проводити навчання персоналу та науковців щодо новітніх методів кібербезпеки та сучасних загроз. Курси з етичного взлому та симуляції кібератак можуть стати ефективними інструментами для підготовки персоналу до реальних сценаріїв.

7. Застосування систем, що реагують на запитання в реальному часі, може значно підвищити швидкість реакції наукових інститутів на кіберзагрози. Ці системи автоматично сповіщають та активують необхідні заходи в разі виявлення аномалій чи потенційно небезпечної активності.

Розробка адаптивних заходів захисту є критичним завданням у світі постійно зростаючих кіберзагроз. У контексті наукових досліджень, де конфіденційність та цілісність даних є найважливішими, використання передових технологій та інноваційних стратегій захисту є вимогою часу. Адаптивні заходи захисту дозволяють ефективно протистояти еволюції кіберзагроз та забезпечують надійний захист цифрової екосистеми наукового середовища.

Загалом, адаптивні заходи захисту наукових досліджень від кібератак визначають майбутнє цифрового наукового середовища, де безпека та конфіденційність інформації стають пріоритетними завданнями. Розробка і впровадження цих заходів дозволять забезпечити стійкість та безпеку наукового співтовариства в умовах постійно зростаючого обсягу кіберзагроз. А постійне вдосконалення стратегій кібербезпеки в умовах динамічного цифрового середовища та активного впровадження інновацій забезпечить стійкий захист від сучасних кіберзагроз.

Література

1. Биков, В. Ю., Буров, О. Ю., & Дементієвська, Н. П. (2019). Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання, (70,№ 2), 313-331.

2. Половенко, Л., & Мерінова, С. (2023). Ймовірнісно-статистичні методи у виявленні кіберінцидентів: інноваційні підходи. Наука і техніка сьогодні, (12 (26)).

3. Корченко, А. О. (2019). Методи ідентифікації аномальних станів для систем виявлення вторгнень.

4. Тихомиров, О. О. (2012). Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: об’єкти і суб’єкти. Інформаційна безпека людини, суспільства, держави, (2), 9.

5. Фурашев, В. М. (2012). Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право, (2 (5)), 162-169.

УДК 004.312.26

ПОНЯТТЯ ПРО ТЕХНОЛОГІЮ СУЧАСНОЇ КВАНТОВОЇ КРИПТОГРАФІЇ

Ніжегородцев Владислав, Пивоваров Володимир
Державний податковий університет (м. Ірпінь)

Анотація. У сфері кібербезпеки квантова криптографія дозволяє розв'язати низку важливих криптографічних задач. Квантові обчислення представляють собою потужну технологію з потенціалом змінити криптографію у засобах кібербезпеки. завдяки своїй здатності квантові обчислення вирішувати проблеми розкладання на множники та пошуку простих чисел набагато швидше, ніж класичні комп'ютери.

Ключові слова: квантові обчислення, криптографія, безпека інформації, кібербезпека.

Abstract. In the field of cyber security, quantum cryptography allows solving a number of important cryptographic problems. Quantum computing is a powerful technology with the potential to revolutionize cryptography in cybersecurity. due to its ability to solve problems of factorization and finding prime numbers, quantum computing is much faster than classical computers.

Key words: quantum computing, cryptography, information security, cyber security.

Квантові обчислення є однією з найбільш футуристичних галузей сучасної науки та технології, яка обіцяє змінити парадигми обчислень в надзвичайно багатьох галузях життя. Дві з найбільш обіцяючих областей застосування квантових обчислень - це криптографія та медицина.

Класичні комп’ютери стають все більш потужними, існують фізичні обмеження на зростання їх продуктивності, цю проблему можна вирішити з використанням квантових комп’ютерів. Сучасні комп’ютери нездатні розв’язати деякі важливі задачі, такі як, наприклад, моделювання квантово-механічних систем. Крім того, існують задачі, які можуть бути розв’язані лише з використанням квантових обчислень [1, с.24].

У сфері кібербезпеки існує поняття квантової криптографії. Йдеться про те, щоб створити нові протоколи безпеки, які майже неможливо зламати. Вже зараз є спеціальні лінії зв’язку, в яких інформація захищена спеціальним квантовим шифруванням.

Методи квантової криптографії забезпечують високий рівень безпеки, але вони все ж є уразливими до багатьох атак, як пасивних, так і активних, що обумовлені різними причинами. Усвідомлення цього положення висунуло вимогу структуризації всього наявного набору методів несанкціонованого проникнення в системи квантової криптографії, що виникли у ході їхнього пошуку розроблювачами квантових криптографічних протоколів [2].

Перевага квантової криптографії полягає в тому, що вона дозволяє розв'язати низку важливих криптографічних задач, для яких доведена неможливість розв'язку за допомоги лише класичної (тобто, неквантової) комунікації. Зокрема, квантова механіка гарантує, що вимірювання певної квантової величини збурює її, що може бути використано для виявлення втручання сторонньої особи до процесу квантового розподілу ключа.

Найкраще розроблений метод квантової криптографії - це квантовий розподіл ключа, який описує процес застосування квантової комунікації для створення та обміну секретним ключем між двома користувачами (яких в теорії інформації традиційно називають Алісою і Бобом) без можливості втручання третьої сторони (Єви), що прагне перехопити інформацію про ключ.

Квантові обчислення представляють собою потужну технологію з потенціалом змінити криптографію у засобах кібербезпеки. У криптографії, квантові обчислення можуть стати загрозою для сучасних методів шифрування, так як вони можуть зламати криптосистеми, які зараз вважаються надійними, завдяки своїй здатності вирішувати проблеми розкладання на множники та пошуку простих чисел набагато швидше, ніж класичні комп'ютери.

Подальша розробка квантово-стійких алгоритмів шифрування є важливою задачею для забезпечення безпеки інформації у майбутньому. Проте вони також породжують нові виклики і потребують подальших досліджень для забезпечення їх безпеки та використання в повсякденних застосуваннях.

Література

1. Квантові інформаційні системи. Навчальний посібник для спеціальності «Прикладна фізика та наноматеріали» / Карлаш Г.Ю. – Київ: факультет радіофізики, електроніки та комп’ютерних систем Київського національного університету імені Тараса Шевченка, 2018. – 77 с.

2. Limar I., Classification of the attacks on quantum systems for the transfer of confidential data/ I. Limar, Ye.Vasiliu, O.Riabukha, T. Zhmurko // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 3, p.181-189.

УДК 004.056.53

ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ ПІДХОДУ “БЕЗПЕКА ЯК КОД” В ХМАРНИХ СЕРЕДОВИЩАХ

Опірський Іван, Вахула Олександр
Національний університет “Львівська політехніка”, м. Львів

Анотація: “Безпека як код” – це підхід організації безпеки в хмарних середовищах, який полягає на методі інтеграції контролів безпеки, політик та кращих практик безпосередньо в процеси розробки та розгортання програмного забезпечення. Дана теза конференції розглядає принципи підходу «Безпека як код”, приклад реалізації, переваги даного підходу та подальші кроки дослідження.

Ключові слова: безпека як код, інфраструктура як код, DevSecOps, DevOps, хмарні середовища, цикл розробки програмного забезпечення.

Abstract: "Security as Code" is an approach to organizing security in cloud environments that involves integrating security controls, policies, and best practices directly into the software development and deployment processes. This conference thesis explores the principles of the "Security as Code" approach, provides an implementation example, highlights the benefits of this approach, and outlines future research directions.

Keywords: security as code, infrastructure as code, DevSecOps, DevOps, cloud environments, software development lifecycle.

Організація безпеки в хмарних середовищах методом “безпека як код”. Більшість споживачів хмарних послуг згідні, з тим, що "Інфраструктура як код" (IaC) дозволяє швидко розгортати послуги в хмарі без ручної конфігурації і, відповідно, помилок. "Безпека як код" йде далі, визначаючи безпечні політики, стандарти і передові практики програмно, щоб їх можна було використовувати за замовчуванням у скриптах конфігурації, які використовуються для налаштування хмарних сервісів і систем. IT-відділи можуть перейти від вічного балансу між бізнес-гнучкістю і безпекою до реалізації того, що ці елементи можна поєднати для надання відповідного рівня обох без жертвування будь-яким із них.
Давайте розглянемо спрощений приклад (рисунок 1):

Рисунок 1 – Спрощена схема реалізації підходу “Безпека як код”

Організаційні політики містять список обов'язкових засобів безпеки. Засоби безпеки розбиваються на правила, які перетворюються в код, зрозумілий централізованою службою перевірки відповідності. Пізніше правила групуються в політики, організовані ієрархічно і визначені структурою успадкування. Служба централізованої перевірки відповідності служить умовною “брамою”, де перевіряється код інфраструктури на відповідність ресурсам, які мають бути розгорнуті відповідно до визначених політик. [4, 5]

Політики можуть бути отримані зі стандартів, регуляцій, передових практик та рекомендацій, включаючи зовнішні установи, такі як: Cloud Security Alliance (CSA); Center for Internet Security (CIS); NIST; GDPR; HIPAA; PCI DSS; У більшості випадків ці вимоги та рекомендації можна визначити у вигляді коду, який може служити запобіжним, виявляючим та реактивним засобом контролю.

Запит на створення ресурсів описаний декларативним способом інфраструктура як код (IaC) - це передумова перед статичною перевіркою відповідності політиці. IaC може бути реалізовано за допомогою інструментів, таких як CloudFormation для AWS, Deployment management для GCP або Resource Manager для Azure, а для більш універсального рішення - Terraform або Pulumi. Статичні перевірки політики слід інтегрувати в CI/CD конвеєр інфраструктурного коду та дотримуватися кращих практик GitOps, щоб уникнути встановлення помилкових конфігурацій та виправити неузгодженості на ранньому етапі.

Компонент служби перевірки відповідності політики може бути реалізований за допомогою Open Policy Agent (OPA) або Regula, обидва є відкритими програмами. В Cloud Native Computing Foundation (CNCF) OPA було прийнято як проект, що перебуває на етапі інкубації у квітні 2019 року, а потім виведено на етап завершення зрілості, 29 січня 2021 року. Він забезпечує єдиний фреймворк для виконання політики по всьому стеку. OPA дозволяє розділити рішення політики від ваших служб, API та мікросервісів і управляти політиками окремо від коду вашого додатка. OPA може бути використаний в управлінні API для декларативного визначення та виконання політики на різних рівнях. [6, 7]

Можна виділити наступні основні технологічні принципи для SaC, які є обов’язковою передумовою для реалізації даного підходу:

• **Автоматизація**: "Безпека як код" ґрунтується на автоматизації для послідовної та масштабованої реалізації політик безпеки. Це включає в себе автоматизоване впровадження засобів безпеки, виявлення вразливостей та усунення проблем.

• **Контроль версій**: "Безпека як код" слід розглядати як програмний код та керувати його в межах системи керування версіями. Це забезпечує чіткий історію змін, сприяє співпраці між командами та дозволяє тестувати зміни в контрольованому середовищі перед впровадженням у виробництво.

• **Повторне використання:** "Безпека як код" повинна бути модульною та спроектованою для повторного використання. Це дозволяє різним командам використовувати та обмінюватися стандартизованими компонентами та конфігураціями засобів безпеки, зменшуючи час та зусилля, необхідні для впровадження безпеки.

• **Відкриті стандарти**: "Безпека як код" повинна базуватися на відкритих стандартах. Це забезпечує більш гнучкий та вендор-незалежний підхід, зменшуючи залежність від конкретних постачальників і дозволяючи командам вибирати найкращі рішення для різних випадків використання.

Висновки

"Безпека як код" є технікою, яка інтегрує безпеку та розробку програмного забезпечення і робить їх невід'ємними елементами. Організації можуть автоматизувати, інтегрувати та здійснювати заходи безпеки протягом життєвого циклу ресурсів хмари, розглядаючи політику безпеки, контролі та найкращі практики як власне код. Дослідження вказує, що "Безпека як код" може бути еволюційним стрибком, а не просто технологічним зрушенням. Це підштовхує до подальшого дослідження спрямованого на виявлення також недоліків даного методу та пропозицій покращення а також аналіз можливостей та практичності його застосування до широкого спектру хмарних сервісів та гібридних реалізацій інфраструктури.

Література

1. Rakesh Kumar, Rinkaj Goyal (2020). Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC) (https://www.sciencedirect.com/science/article/abs/pii/S0167404820302406)

2. Kim Carter (2017). Francois Raynaud on DevSecOps https://ieeexplore.ieee.org/document/8048652

3. Sarthak Das (2023). Security as Code 1st Edition

4. Chhavi Adtani, Aaron Bawcom, Jan Shelly Brown, Rich Cracknell, Rich Isenberg, Kaz Kazmier, Pablo Prieto-Munoz, and David Weinstein (2022). Security as code: The best (and maybe only) path to securing cloud applications and systems (https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/security-as-code-the-best-and-maybe-only-path-to-securing-cloud-applications-and-systems)

5. Xuejiao Zhang (2021). Cloud governance and compliance on AWS with policy as code (https://aws.amazon.com/ru/blogs/opensource/cloud-governance-and-compliance-on-aws-with-policy-as-code/)

6. Xuejiao Zhang (2020). Compliance as code and auto-remediation with Cloud Custodian

7. Fausto Lendeborg (2021). Security as Code is the Future to Governing Risk (https://cloudsecurityalliance.org/blog/2021/10/19/security-as-code-is-the-future-to-governing-risk/

УДК 681.3.05

ВИКОРИСТАННЯ ШИФРУ ХІЛЛА В КРИПТОЛОГІЇ

Пахарчук Максим, Кусій Мирослава
Львівський державний університет безпеки життєдіяльності

Анотація. Розглянуто особливості та алгоритм використання шифру Хілла для зашифрування і дешифрування тексту. Розглянуто використання шифру Хілла на конкретному прикладі. Встановлено, що, методи класичної криптографії гарантують захист інформації тільки тоді, якщо використано ефективний криптографічний алгоритм, а також будуть дотримуватись умови секретності та цілісності ключів шифрування.

Ключові слова: шифр Хілла, захист інформації, шифрування/дешифрування, матриця, ключ, крипто текст

Abstract. The features and algorithm of using the Hill cipher for encryption and decryption of text are considered. The use of the Hill cipher on a specific example is considered. It is established that the methods of classical cryptography guarantee the protection of information only if an effective cryptographic algorithm is used, and the conditions of secrecy and integrity of encryption keys are met.

Keywords: Hill cipher, information protection, encryption/decryption, matrix, key, cryptotext

В сучасному світі різко зріс і продовжує зростати об'єм конфіденційної інформації, яка передається по відкритих каналах зв'язку. Тому проблема захисту інформації є дуже актуальною.

Криптологія – це галузь науки, яка вивчає методи захисту інформації від несанкціонованого доступу, включаючи шифрування (криптографію) та дешифрування (криптоаналіз). Термін «криптологія» походить від грецьких слів «kryptos» (прихований) і «logos» (слово), що вказує на отримання інформації. Існує багато методів захисту інформації. Серед класичних – це Афінна система підставлянь Цезаря, як продовження її – криптографічна система Лестера Хілла. Шифр Хілла – це криптографічний алгоритм, який використовується для шифрування та дешифрування повідомлень. Основна ідея полягає в тому, щоб використовувати матриці для перетворення блоків символів у відкритому тексті в блоках шифротексту і навпаки.

Відкрите повідомлення при такому шифруванні розбивається на $k-$грами. Кожній $k-$грамі ставимо у відповідність вектор X (тобто матриця розміру $k\times 1)$. Криптотекст задається з допомогою *ключа* $A\in GL_k(\square_N)$, де $GL_k(\square_N)-$це множина оборотних матриць розміру $k\times k$ з коефіцієнтами з кільця $\square_N \overset{df}{=} \square / N\square$, де $N-$число букв алфавіту, яким

користується відправник (для українського алфавіту $N = 33$, якщо не враховані пробіли чи розділові знаки).

Шифрування: З допомогою необоротної над $\mathbb{Z}_N$ матриці A знайдемо криптотекст $C = AX = X'$.

Дешифрування: $D(X') = D(AX) = A^{-1}X' = A^{-1}AX = X$, тобто дешифрування здійснюється з допомогою оберненої до матриці A над кільцем $\mathbb{Z}_N$ матриці A^{-1}.

Розглянемо докладніше випадок $k = 2$, тобто біграмний лінійний шифр. В якості ключа виберемо довільну матрицю

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}_N \qquad (1)$$

з $\det A \neq 0$ і $\text{НСД}(\det A, N) = 1$.

Приклад. Нехай потрібно зашифрувати з допомогою біграмного лінійного шифру сполучення слів «Пройдіть в укриття» з ключем $A = \begin{pmatrix} 1 & 16 \\ 2 & 1 \end{pmatrix}$

Розв'язання. Поставимо у відповідність біграмам «ПР», «ОЙ», «ДІ», «ТЬ», «ВУ», «КР», «ИТ», «ТЯ» вектори, використовуючи табл.1.

Табл.1

А 0	Б 1	В 2	Г 3	Ґ 4	Д 5	Е 6	Є 7	Ж 8	З 9	И 10
І 11	Ї 12	Й 13	К 14	Л 15	М 16	Н 17	О 18	П 19	Р 20	С 21
Т 22	У 23	Ф 24	Х 25	Ц 26	Ч 27	Ш 28	Щ 29	Ь 30	Ю 31	Я 32

«ПР» $\longrightarrow \begin{pmatrix} 19 \\ 20 \end{pmatrix}$ «ОЙ» $\longrightarrow \begin{pmatrix} 18 \\ 13 \end{pmatrix}$ «ДІ» $\longrightarrow \begin{pmatrix} 5 \\ 11 \end{pmatrix}$ «ТЬ» $\longrightarrow \begin{pmatrix} 22 \\ 30 \end{pmatrix}$

«ВУ» $\longrightarrow \begin{pmatrix} 2 \\ 23 \end{pmatrix}$ «КР» $\longrightarrow \begin{pmatrix} 14 \\ 20 \end{pmatrix}$ «ИТ» $\longrightarrow \begin{pmatrix} 10 \\ 22 \end{pmatrix}$ «ТЯ» $\longrightarrow \begin{pmatrix} 22 \\ 32 \end{pmatrix}$

Отримаємо відкритий текст: $\begin{pmatrix} 19 & 18 & 5 & 22 & 2 & 14 & 10 & 22 \\ 20 & 13 & 11 & 30 & 23 & 20 & 22 & 32 \end{pmatrix}$

Знайдемо криптотекст, використовуючи ключ A. Отримаємо:

$$\begin{pmatrix}1 & 16\\ 2 & 1\end{pmatrix}\cdot\begin{pmatrix}19 & 18 & 5 & 22 & 2 & 14 & 10 & 22\\ 20 & 13 & 11 & 30 & 23 & 20 & 22 & 32\end{pmatrix}$$
$$=\begin{pmatrix}9 & 28 & 16 & 7 & 7 & 4 & 32 & 6\\ 25 & 16 & 21 & 8 & 27 & 15 & 9 & 10\end{pmatrix}$$

Отже, криптотекст – це стовпці матриці:

$$\begin{pmatrix}9 & 28 & 16 & 7 & 7 & 4 & 32 & 6\\ 25 & 16 & 21 & 8 & 27 & 15 & 9 & 10\end{pmatrix}$$

Відповідні біграми за таблицею 1 – наступні: «ОЦ», «ХІ», «ЄЧ», «ПМ», «ШЛ», «ТС», «КС», «СР». Таким чином, одержувач отримав шифрований текст «ОЦХІЄЧПМШЛТСКССР».

Далі одержувач хоче розшифрувати його. Для цього потрібно знайти обернену до A матрицю за правилами лінійної алгебри. Така матриця існує, оскільки вона оборотна. Знайдемо *det A = 1-32(mod 33) = -31(mod 33) = 2* НСД *(2,33)=1*

Тому $A^{-1} = 2^{-1}\begin{pmatrix}1 & -16\\ -2 & 1\end{pmatrix} = 2^{-1}\begin{pmatrix}1 & 17\\ 31 & 1\end{pmatrix}$ (mod 33)

Знайдемо 29^{-1} використовуючи ділення з остачею

$$33 = 2\cdot 16 + 1 \Rightarrow 1 = 33 - 2\cdot 16$$

Звідки отримуємо $2^{-1} = -16(mod\ 33) = 17(mod\ 33)$

Тому $A^{-1}=\begin{pmatrix}17 & 25\\ 32 & 17\end{pmatrix}(mod\ 33)$

Маємо:

$$\begin{pmatrix}17 & 25\\ 32 & 17\end{pmatrix}\cdot\begin{pmatrix}9 & 28 & 16 & 7 & 7 & 4 & 32 & 6\\ 25 & 16 & 21 & 8 & 27 & 15 & 9 & 10\end{pmatrix} =$$
$$\begin{pmatrix}19 & 18 & 5 & 22 & 2 & 14 & 10 & 22\\ 20 & 13 & 11 & 30 & 23 & 20 & 22 & 32\end{pmatrix}$$

Отже, ми прийшли до відкритого тексту «Пройдіть в укриття».

Література

1. М.Ф.Стасюк Математичні основи криптографії (спеціальні розділи математики). Навчальний посібник. ЛДУБЖД. Львів. –2021.

2. О.В.Вербіцький Вступ до криптології / О.В. Вербіцький. –Львів.: ВНТЛ, 1998. –246с.

3. Грицюк П.Ю. Афінні перетворення у криптографічній системі Лестера Хілла / П.Ю. Грицюк // 66-а науково-технічна студентська конференція НЛТУ України. – Серція: Інформа- ційні технології : результати 66-ої СНТК, м. Львів, 13 листопада 2014 р. – Львів : НЛТУ України. [Електронний ресурс]. – Доступний з http://it.nltu.edu.ua/index.php/kafedra/news/286-rezultaty-66- oi-snk-sektsiia-informatsiini-tekhnolohii

4. Ємець В. Сучасна криптографія: Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів : Вид-во БаК, 2003. – 144 с

УДК 004.056

РОЗРОБЛЕННЯ МОДЕЛІ ТЕХНІЧНОГО ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ

Полотай Орест, Дубик Анастасія-Оксана
Львівський державний університет безпеки життєдіяльності,
Національний університет "Львівська політехніка"

Описано важливість вивчення та поглиблення знань з розробки моделей технічного захисту мережевої інфраструктури організацій.
Ключові слова: захист мережі, Cisco Packet Tracer, моделі захисту

Describes the importance of studying and deepening knowledge on the development of models of technical protection of the network infrastructure of organizations.
Key words: network protection, Cisco Packet Tracer, protection models

У сучасному цифровому світі, де інформація є ключовим ресурсом, а технологічний прогрес зростає експоненційно, питання безпеки мережевої інфраструктури стає надзвичайно актуальним та невідкладним. Кіберзагрози, що небезпечно еволюціонують, стають викликом для надійності та конфіденційності інформації, яка обробляється в мережевих системах. Від традиційних атак до вдосконалених методів кіберзлочинців, мережеві інфраструктури стають об'єктом зростаючого інтересу та загроз.

Мережева інфраструктура – це сукупність різного устаткування, а також програмного забезпечення, яка формує особливе середовище для ефективного процесу обміну даними, а також для роботи бізнес-додатків.

За допомогою мережевої інфраструктури організації обмінюються даними та пов'язують всі робочі IT-елементи. Мережева інфраструктура може сильно відрізнятися з точки зору:

- розміру покривається території;
- кількості підключених користувачів;
- кількості та видів доступних послуг.

Мережева інфраструктура складається з:

- активного обладнання (комутатори, маршрутизатори й т.д.);
- пасивних пристроїв (кабелі, кабельні канали, монтажні шафи, комутаційні панелі, розетки інформаційного типу);
- периферійних комп'ютерів і обладнання (ксерокси, робочі станції, сервери, принтери та сканери);
- програмного забезпечення для управління та моніторингу мережевої інфраструктури.

Важливо вміти розробляти моделі технічного захисту мережевої інфраструктури організації. Вивчення сучасної техніки та методів захисту, спрямованих на запобігання та виявлення кібератак, забезпечуючи високий рівень безпеки, є дуже важливим для забезпечення неперервності бізнес-процесів та дотримання вимог конфіденційності.

У цьому контексті, потрібно розглядати важливі аспекти впровадження технічного захисту, включаючи аналіз поточних загроз, ідентифікацію слабких місць в мережевій інфраструктурі, розробку ефективних стра-

тегій захисту, та впровадження сучасних технологій кібербезпеки. Метою таких вивчень є не лише надання вичерпного огляду сучасних викликів та загроз у сфері кібербезпеки, але і розробка конкретної моделі захисту, яка забезпечить ефективний контроль та реагування на потенційні атаки.

Вивчення цієї теми є ключовим елементом підготовки фахівців з інформаційної безпеки та технічних спеціалістів. Розуміння та вдосконалення заходів технічного захисту мережевої інфраструктури визначають успішність організацій у високотехнологічному середовищі. Під час вивчення цієї теми, важливо навчитися розкривати важливі аспекти та внесок власний внесок у сферу кібербезпеки, сприяючи створенню більш захищеної та надійної мережевої інфраструктури для організацій.

Безумовно, вивчення теми "Розроблення моделі технічного захисту мережевої інфраструктури організації" має величезну важливість у сучасних умовах технологічного розвитку та поширення кіберзагроз. Зростання обсягу цифрової інформації, яка зберігається та обробляється в мережевій інфраструктурі, підвищує загрози з боку кіберзлочинців, які можуть намагатися незаконно отримати доступ до цих даних. Зростання кількості та складності кібератак, включаючи вимагання викупу, розповсюдження вірусів та шкідливих програм, підкреслює необхідність розробки та вдосконалення технічних заходів безпеки. Захист важливих корпоративних даних та конфіденційної інформації є вирішальним для уникнення фінансових втрат, порушень законодавства про конфіденційність та збереження репутації організації. Вдосконалені технічні засоби захисту дозволяють підтримувати неперервність бізнесу, забезпечуючи стабільну роботу мережевої інфраструктури навіть під час потенційних кібератак або природних катастроф. Організації повинні відповідати регулятивним вимогам щодо захисту даних та конфіденційності, і технічний захист мережевої інфраструктури є ключовим елементом для виконання цих вимог. Захист мережевої інфраструктури є необхідним для безпечного впровадження нових технологій, таких як хмарні обчислення, Інтернет речей (IoT) та штучний інтелект, що вимагає вдосконаленої кібербезпеки.

Отже, вивчення та розробка моделі технічного захисту мережевої інфраструктури стає критичним етапом для забезпечення безпеки, стійкості та довіри в сучасних корпоративних та технологічних середовищах.

Література

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

2. Полотай О, Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи. Захист інформації вінформаційнокомунікаційних системах : зб. тез. III Всеукр. наук.-практ.конф. Молодих учених, студентів і курсантів. Львів, ЛДУ БЖД. – 2019. С.76-78.

3. Полотай О., Мороз Ю., Великий В. Методи технічного захисту інформації у сфері інформаційної безпеки. Інформаційна безпека інформаційні технології: Збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. – Львів, 2020. – С. 40-41.

УДК 654.01

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В 5G МЕРЕЖАХ

Полотай Орест, Нагірний Ростислав
Львівський державний університет безпеки життєдіяльності, м. Львів,
Національний Університет «Львівська політехніка»

Описано особливості інформаційної безпеки сучасних технологій 5G-мереж.
Ключові слова: інформаційна безпека, 5G-мережі

Features of information security of modern 5G network technologies are described.
Keywords: information security, 5G networks

5G – це п’яте покоління мобільних мереж, новий етап розвитку технологій, який покликаний розширювати можливості доступу до Інтернету через мережі радіодоступу, пропонує надійніші з'єднання на смартфонах та інших пристроях, ніж будь-коли раніше.

Найбільша відмінність між мережами 5G і мережами попередніх поколінь – це вища швидкість мережі Інтернет. Теоретично можливі швидкості становлять 10-20 Гбіт/с, при цьому затримка передачі сигналу становить лише 1-2 мс. Наприклад, теоретична максимальна швидкість для 4G становить до 1 Гбіт/с із затримкою сигналу 10 мс, а для 3G - до 42 Мбіт/с із часом відгуку 100 мс.

Безпека в 5G – це захищеність інформації та допоміжної інфраструктури від випадкових або навмисних природних або антропогенних впливів, які можуть завдати шкоди власникам і користувачам інформації та допоміжної інфраструктури.

Поняття безпеки в 5G, як і захист інформації, є комплексним питанням, яке реалізується через впровадження систем безпеки. Питання захисту інформації є багатогранним і складним і включає в себе ряд ключових проблем.

Основними загрозами в 5G мережах є:

- Загрози пов'язані з навколишнім середовищем (стихійні лиха, техногенні катастрофи і т.д.);
- Технічні (відмови обладнання і програмного забезпечення, витік інформації по каналах зв'язку і т.д.);
- Людські (в результаті навмисних і ненавмисних дій).

Як і будь-яка масштабна технологія, 5G приверне увагу хакерів і кіберзлочинців.

Концепція безпеки мереж 5 п'ятого покоління включає в себе:

- Автентифікацію користувача з боку мережі.
- Автентифікацію мережі з боку користувача.
- Узгодження криптографічних ключів між мережею і призначеним для користувача обладнанням.
- Шифрування і контроль цілісності сигнального трафіку.
- Шифрування і контроль цілісності призначеного для користувача трафіку.
- Захист ідентифікатора користувача.
- Захист інтерфейсів між різними елементами мережі відповідно до концепції мережевого домену безпеки.
- Ізоляцію різних верств механізму network slicing і визначення для кожного шару власних рівнів безпеки.
- Автентифікацію користувача і захист трафіку на рівні кінцевих сервісів (IMS, IoT та інших).

Безпека телекомунікаційних мереж визначається наступними елементами

- Стандартизація: процес, за допомогою якого оператори, постачальники та інші зацікавлені сторони встановлюють стандарти для спільної роботи мереж у всьому світі. Сюди входить і те, як найкраще захистити мережу та її користувачів від зловмисників.
- Проектування мережі: проектування, розробка та впровадження постачальниками мережі узгоджених стандартів для функціональних мережевих елементів і систем, які відіграють ключову роль у забезпеченні функціональності та безпеки кінцевого мережевого продукту.
- Це відіграє ключову роль у встановленні параметрів безпеки та подальшому підвищенні безпеки та стійкості мережі.
- Розгортання та експлуатація мережі. Операційні процеси, які дозволяють мережі функціонувати і забезпечувати цільовий рівень безпеки, сильно залежать від розгортання і роботи самої мережі. Тому для ефективного захисту потоків даних в мережі необхідно використовувати новітні технології, в тому числі продукти Cisco Systems.

Мережі 5G пропонують вищі швидкості, ніж їхні попередники, що може допомогти зменшити затримку та забезпечити більш безпечну передачу даних. Ця покращена швидкість забезпечує міцну основу для розробки більш безпечних служб, таких як хмарні служби. Мережі 5G також забезпечують більш безпечний зв’язок між пристроями завдяки покращеним протоколам шифрування та покращеним механізмам автентифікації. Цей покращений захист допомагає зловмисникам ускладнити доступ до мереж і компрометувати дані.

5G також підтримує розвиток нових технологій, таких як Інтернет речей (IoT). Використання пристроїв IoT збільшує поверхню атаки мережі, роблячи її більш уразливою до кібератак. Мережі 5G можуть допомогти захистити ці пристрої, надаючи розширені протоколи шифрування та автентифікації. Мережі 5G також забезпечують більш розширені заходи безпеки, такі як технології розподіленої книги, які можна використовувати для захисту передачі даних.

Мережі 5G можуть допомогти компаніям захистити свої дані від кібератак, а також дозволити компаніям впроваджувати розширені засоби контролю безпеки, такі як штучний інтелект і машинне навчання, які можуть допомогти швидше виявляти кіберзагрози та реагувати на них. Ця підвищена швидкість і надійність може допомогти захистити компанії від витоку даних, що може коштувати дорого та завдати шкоди їхній репутації.

Підсумовуючи, можна стверджувати, що запровадження мереж 5G трансформує ландшафт цифрової безпеки. Мережі 5G пропонують покращену швидкість, надійність і заходи безпеки, які можуть допомогти захистити бізнес від кібератак. Цей покращений захист може допомогти компаніям захистити свої дані та забезпечити більшу безпеку своїх систем.

Література

1. Наслідки для безпеки 5G-мереж. URL: https://ts2.space/uk/наслідки-для-безпеки-мереж-5g-2/#gsc.tab=0

2. Правило В.В., Кормульов О.С. Методи забезпечення заданих показників безпеки // Збірник матеріалів XIV Міжнародної науково-технічної конференції "Перспективи телекомунікацій 2020". Київ: 2020. С. 178-180.

3. Як захистити 5G від взлому: вивчаємо архітектуру безпеки Хабр URL: https://habr.com/ru/company/trendmicro/blog/453120/

УДК 372.862

ПРОБЛЕМА БЕЗПЕКИ В ІНТЕРНЕТІ ДІТЕЙ ТА ПІДЛІТКІВ

Паздрій Анатолій, Дудикевич Валерій
Національний університет «Львівська політехніка»

Описано проблему недостатнього інформування молоді та дітей в сфері безпечної поведінки в Інтернеті.
Ключові слова: безпека в Інтернеті, освіта.

Describes the problem of insufficient informing of the youth and kids about safe behavior in Internet.
Keywords: Internet safety, education.

У сучасну еру кіберпростору та загальної комп'ютеризації взаємодії з мережею Інтернет стали невід'ємною частиною життя більшості населення цивілізованого світу. В розвинених країнах вже неможливо уявити собі життя без комп'ютерів, смартфонів, планшетів, та інших приладів, що дозволяють як делегувати їм механічну роботу, починаючи з калькулятора в телефонах і закінчуючи веденням фінансової документації, так і отримувати доступ до, здавалось би, безмежної всесвітньої павутини інформації, веб-сторінок, мільйонів різних додатків та сервісів. Усі ми користуємося цими приладами, їхніми перевагами та можливостями. І багато хто не здогадується, що в таких зручних і корисних речей є і темна сторона.

Варто пам'ятати, що мережа Інтернет, і всі її сервіси – не більше, ніж інструмент. Інструменти не є добрими, вони не є злими. Те, який вплив може здійснити інструмент, та які будуть наслідки його застосування, залежить виключно від того, в чиїх руках він опиниться. І хоча хотілось би вірити що всі люди добрі, і будуть використовувати блага технологій лише за призначенням, нажаль, ми живемо в неідеальному світі. Будь-який інструмент може опинитись в руках людини з поганими намірами. І всесвітня павутина Інтернету – не виключення.

Звісно, будь-яка людина, що користується інтернетом, в тій чи іншій мірі наражає себе на небезпеку. Це необхідний ризик, на який доводиться йти, щоб отримувати користь від всіх позитивних аспектів, що пропонує нам Інтернет. Проте, усвідомлювати наявність ризику, та активно протидіяти його реалізації – зовсім різні речі.

Серед користувачів інтернету вже давно ходить доволі песимістична думка, що приватність в Інтернеті – це міф. І, нажаль, дедалі більше інцидентів доводять, що ця думка має право на існування. Все, що потрапляє в Інтернет, в Інтернеті залишиться, і з цим нічого не можна

зробити, наскільки би старанними, багатими чи могутніми Ви б не були. Проте, людина з достатнім усвідомленням цього факту зможе в певній мірі контролювати свій інформаційний потік, та мінімізувати ризик витоку чутливої та/або персональної інформації. Хоча, нажаль, навіть не всі дорослі здатні грамотно управляти своєю інформаційною безпекою.

Але є певна вікова група, що значно більше вразлива до всіх небезпек, що може принести з собою користування Інтернетом, а саме – діти. Згідно статистики UNICEF, приблизно одна з трьох дітей є користувачем мережі Інтернет. І з кожним роком «вік входження» все зменшується і зменшується. Є чимало випадків, коли батьки замість іграшок дають своїм дітям планшет або телефон, наприклад, щоб дивитись мультфільми на YouTube.

В даній доповіді не буде розглядатись питання того, наскільки дітям шкодить сам факт використання електронних приладів в настільки ранньому віці. Конкретно зараз хочеться сконцентрувати увагу на іншому аспекті цієї ситуації – на безпеку користування мережею Інтернет.

Ні для кого не секрет, що Інтернет може бути дуже небезпечним місцем, особливо для необачного користувача. І точно так само загальновідомим фактом є те, що ніхто не народжується зі знаннями про те, як цих небезпек уникати. Розкриття конфіденційної інформації, кібербулінг, небезпечна або небажана інформація – одні з найменш руйнівних проблем, з якими можуть стикнутись діти, що користуються Інтернетом без необхідної підготовки.

Але звідки ця підготовка може взятись? Дуже мало хто з батьків дійсно детально пояснює дітям, які ризики може нести собою Інтернет. Хтось повністю обмежує дітей від мережі, що може створити проблеми в майбутньому, коли вони стикнуться з нею непідготованими. Хтось обмежується звичайним «не розказуй незнайомцям свою домашню адресу». Проте мало хто з батьків має достатній рівень освіти в сфері кібербезпеки щоб підготувати своїх дітей до того, з чим вони можуть стикнутись на просторах всесвітньої павутини.

Але яким ж буде рішення даної проблеми? Як можна вберегти дітей і підлітків від ризиків, з якими вони можуть стикнутись, не покладаючись на відповідальність батьків, які в більшості випадків, навіть при всій старанності, просто не мають необхідної компетенції?

Вирішення такої проблеми вимагає кардинальних змін, і, в першу чергу – в системі освіти. Саме школа, в якій працюють кваліфіковані знавці своїх сфер, повинна готувати дітей до того, з чим вони можуть стикнутись в житті при використанні Інтернету. Цю проблему більше не можна ігнорувати, відкладати на потім, сподіватись, що діти самі розберуться. Не можна більше робити вигляд, що Інтернет – це щось не варте уваги освітян. Інтернет тепер – така сама частина нашого життя, як

математика, економіка, правила дорожнього руху та інші. Шкільний курс інформатики більше не може ігнорувати цю проблему – він має не лише вчити дітей використовувати електронні прилади, він повинен в першу чергу вчити дітей робити це безпечно для себе та оточуючих. Про такі речі, як фішингові сайти, соціальну інженерію, проблеми надлишкової публічності, використання слабких паролів повинні вчити дітей починаючи з того віку, коли вони вже здатні самостійно користуватись Інтернетом в своїх цілях. А цей вік, як показують останні події, настає значно раніше, ніж нам здається.

Таким чином, система освіти в сфері інформаційної безпеки повинна зазнати необхідних змін, оскільки, як показує практика, необережне поводження з інтернетом може бути ледь не настільки ж небезпечним, як перехід дороги на червоне світло. Інтернет та його сервіси став невід'ємною частиною нашого повсякденного життя, включно з наймолодшими членами нашого суспільства, а отже, ризики, з якими можна стикнутись при використанні всесвітньої павутини, не можна більше ігнорувати. Реформування освіти в сторону підвищення цифрової грамотності молоді та обізнаності в сфері власної безпеки в кіберпросторі повинне бути пріоритетним напрямком розвитку системи освіти в наше століття загальної комп'ютеризації.

Література

1. Devorah Heitner. Screenwise. Routledge, 2016
2. Nancy E. Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn To Use the Internet Safely and Responsibly. Jossey-Bass, 2007.
3. Growing Up in a Connected World: Understanding Children's Risks and Opportunities in a Digital Age Веб сайт UNICEF. [Електронний ресурс]: – режим доступу: https://www.unicef-irc.org/growing-up-connected.

УДК 004.056.53

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ УЛЬТРАЗВУКОВОГО МАСКУВАННЯ

Палагін Володимир, Зорін Олександр, Бінецький Олег
Черкаський державний технологічний університет

Розглянуті технічні канали витоку мовної інформації та запропоновано метод, який грунтується на закритті акустичного каналу нав'язуванням на мікрофон закладного пристрою ультразвукової частоти, промодульованої імпульсними сигналами заданої шпаруватості та амплітуди. Даний підхід дозволяє уникнути витоку мовної інформації на основі закладних пристроїв без погіршення якості її циркулювання в приміщенні.

Ключові слова: Витік мовної інформації, ультразвукове маскування.

The technical channels of speech information leakage are considered and a method is proposed, which is based on closing the acoustic channel by imposing an implanted device of ultrasonic frequency on the microphone. The frequency of ultrasonic imposition is modulated by rectangular pulses of a given frequency and amplitude. This approach allows you to avoid the leakage of language information based on embedded devices without deteriorating the quality of its circulation in the room.

Key words: *Leakage of speech information, ultrasonic masking.*

Технічний захист інформації - це комплекс заходів і технічних засобів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, а також на захист інформаційних систем від несанкціонованого доступу, втручань та знищення. Технічний захист є важливою складовою інформаційної безпеки, в тому числі різноманітних каналів витоку мовної інформації, яка залишається ключовою в інформаційному трафіку.

Такі особливості циркулювання мовної інформації, як висока швидкість обміну, можливість індентифікації співрозмовників та їх психологічного портрету, конфіденційність повідомлень роблять її привабливою для викрадення різноманітними сучасними засобами.

Для перехоплення мовної інформації зловмисник може використовувати самий широкий спектр сучасних засобів акустичної розвідки, яка базується на застосуванні портативних закладних пристроїв, спрямованих мікрофонів, електронних стетоскопів, використання різноманітних пристоїв для реалізації витоку завдяки мікрофоному ефекту, застосування оптико-електронних акустичних систем та ін.

Для боротьби з такими каналами витоку пропонуються різноманітні засоби та спеціальні заходи, зокрема встановлення акустичних екранів, використання спеціальних матеріалів та конструкцій, які зменшують роз-

повсюдження звуку і зменшують його витік. Використовують технології активного чи пасивного шумоподавлення з метою зменшення зовнішніх шумів та завдання перешкод для ненавмисного витоку звуку. Застосовують фізичні заходи, такі як контроль доступу, відеоспостереження та інші для запобігання несанкціонованому доступу до приміщень, де обробляється голосова інформація. Окремим напрямом захисту акустичної інформації є її криптографічний захист та використання методів шифрування аудіосигналів для забезпечення конфіденційності та запобігання несанкціонованому прослуховуванню.

Для закриття акустичного каналу витоку через закладні пристрої чи мікрофонний ефект в роботі пропонується застосування технології активного шумоподавлення при застосуванні ультразвукового сигналу, який циркулює в приміщенні. Такий сигнал не заважає співрозмовникам та не створює для них дискомфортних умов, разом з тим унеможливлює роботу прихованих мікрофонів та інших пристроїв. Для підвищення ефективності активного шумоподавлення ультразвуковий сигнал піддається модуляції прямокутними сигналами певної шпаруватості та амплітуди. Такий підхід підвищує захист мовної інформації в приміщенні від різноманітних каналів витоку.

УДК 004.056.5:621.391.71

МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ АВТОМАТИЗОВАНИХ СИСТЕМ МОНІТОРИНГУ ВИРОБНИЧИХ ПРОЦЕСІВ

Пановик Уляна, Довганик Денис, Гідей Роман
Українська академія друкарства,
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. Розглядається важливий аспект сучасних технологій – метрологічне забезпечення захисту інформації в автоматизованих системах моніторингу виробничих процесів. Зосереджуючись на визначенні та функціях метрологічного забезпечення, а також на законодавчій та нормативній основі України, публікація покликана підкреслити важливість збалансованого підходу до кібербезпеки в промислових процесах.

Ключові слова: метрологічне забезпечення, кібербезпека, автоматизована система моніторингу.

Abstract. An important aspect of modern technologies is the metrological provision of information protection in automated systems for monitoring production processes. Focusing on the definition and functions of metrological support, as well as on the legislative and regulatory framework of Ukraine, the publication is designed to emphasize the importance of a balanced approach to cybersecurity in industrial processes.

Keywords: metrological support, cybersecurity, automated monitoring system.

Промислова автоматизація та системи моніторингу включають різновиди систем, таких як наглядовий контроль та збір даних, а також розподілені системи управління. Ці системи отримують дані з промислових процесів за допомогою специфічних пристроїв, таких як програмні логічні контролери, віддалені блоки-термінали та інші інтелектуальні електронні пристрої, і взаємодіють із даними виробничих процесів.

У цьому контексті нові рішення, що базуються на парадигмі віддалених обчислень, дають можливість дослідникам використовувати сервісноорієнтовані інтерфейси архітектури, які реалізують зв’язок інфраструктури інформаційних та комунікаційних технологій із різними пристроями (датчики виробництва, розумні лічильники, радіочастотні ідентифікатори, смартфони) за допомогою бездротового підключення. Це забезпечує точний потік інформації в реальному часі, покращуючи процеси автоматизації в термінах операцій і водночас підсилює заходи безпеки для збереження цілісності та конфіденційності інформації.

На сьогодні актуальним є питання забезпечення точності вимірювань параметрів небезпечних та завадових сигналів під час контролю технологічних процесів. Оскільки діяльність, що пов’язана з технічним захистом інформації, регулюється законодавством у сфері метрології, то виникає необхідність у формуванні чіткого визначення ключових аспектів метрологічної діяльності в галузі захисту інформації.

Метрологічне забезпечення захисту інформації в автоматизованих системах моніторингу виробничих процесів визначається як система заходів, спрямованих на забезпечення достовірності та цілісності інформації, яка використовується в цих системах. Головним завданням метрологічного забезпечення є надання впевненості в точності та достовірності вимірювань, а також управління ризиками, пов'язаними з можливим порушенням безпеки інформації. На підприємствах та в організаціях, що виконують роботи у сфері забезпечення технічного захисту інформації, обов'язково утворюються метрологічні служби або призначаються особи, відповідальні за забезпечення єдності вимірювань. Основні функції метрологічних служб організацій та підприємств охоплюють розроблення та впровадження стандартів безпеки, моніторинг та аналіз загроз, а також надання рекомендацій із покращення систем безпеки. Метрологічне забезпечення також передбачає регулярні перевірки та калібрування засобів вимірювань, що використовуються в системах.

Законодавча основа метрологічного забезпечення в Україні визначається низкою нормативних актів, спрямованих на забезпечення стандартів та вимог щодо захисту інформації. Стаття 3 Закону України «Про метрологію та метрологічну діяльність» визначає сферу законодавчо регульованої метрології як вид діяльності, що пов'язаний зі здійсненням робіт із технічного захисту інформації. Це означає, що всі види робіт, які спрямовані на забезпечення технічного захисту інформації, підпадають під законодавчо регульовану метрологію. Для забезпечення єдності вимірювань проводиться державне регулювання у сфері вимірювань, одиниць вимірювання та засобів вимірювальної техніки. Результати вимірювань можуть використовуватися в рамках законодавчо регульованої метрології, якщо вони відповідають відомим характеристикам похибок або невизначеності вимірювань.

Методи вимірювань, які використовують для технічного захисту інформації, визначаються в нормативно-правових актах або відповідних нормативних документах, на які є відповідні покликання в нормативно-правових актах, доступних на офіційному вебсайті Державної служби спеціального зв'язку та захисту інформації України [1, 2]. Додатково, є спеціальні нормативи у сфері кібербезпеки, які регулюють заходи з захисту інформації в автоматизованих системах. У галузі забезпечення технічного захисту інформації використовуються засоби вимірювальної техніки, які підлягають законодавчому регулюванню і мають відповідати вимогам точності, встановленим для цих засобів, за визначених умовах експлуатації. Законодавчо регульовані засоби вимірювальної техніки, які використовуються в роботах із забезпечення технічного захисту інформації, підлягають метрологічному нагляду. Під час метрологічного нагляду за такими засобами проводиться перевірка: стану та дотримання правил застосування засобів вимірювань; відповідності вимогам щодо періодичної повірки засобів вимірювань; використання дозволених одиниць вимірювання під час експлуатації засобів вимірювань. Нормативна основа метрологічного забезпечення у сфері кібербезпеки України охоплює стандарти та вимо-

ги до технічних засобів, програмного забезпечення та процесів, що забезпечують захист інформації [3]. З огляду на швидкий темп розвитку технологій та зростання загроз кібербезпеки, постійне оновлення та вдосконалення метрологічного забезпечення залишається важливим завданням для підтримання безпеки виробничих процесів [4].

Отже, забезпечення метрологією в галузі кібербезпеки містить комплекс організаційно-технічних заходів, спрямованих на забезпечення єдності та необхідної точності вимірювань параметрів небезпечних та завадових сигналів під час контролю захисних процесів для інформації. Це також передбачає забезпечення ефективності захисту інформації, розроблення сучасних методів вимірювань та технічних засобів для зменшення ризиків витоку інформації та підвищення якості робіт із захисту інформації. Метрологічне забезпечення цієї галузі включає всі етапи життєвого циклу захисту інформації, розпочинаючи з науково-дослідних та експериментально-конструкторських робіт. Ці етапи включають аналіз стану вимірювань, контролю та випробувань; встановлення оптимальної номенклатури вимірювальних величин та використання засобів вимірювань відповідної точності; проведення повірки та калібрування засобів вимірювань; розроблення методів виконання вимірювань для забезпечення встановлених норм точності; здійснення метрологічної експертизи конструкторської і нормативно-технічної документації; оцінку технічної компетентності та проведення метрологічного нагляду за законодавчо регульованими засобами вимірювань. Узагальнюючи, метрологічне забезпечення захисту інформації в автоматизованих системах моніторингу виробничих процесів є критично важливим аспектом у сучасному промисловому середовищі. Забезпечення стандартів та вимог безпеки, спрямованих на захист інформації, допомагає уникнути можливих загроз та зберегти надійність автоматизованих систем.

Література

1. Перелік актів законодавства у сфері технічного захисту інформації Держспецзв’язку. URL: https://cip.gov.ua/ua/news/perelik-aktiv-zakonodavstva-u-sferi-tekhnichnogo-zakhistu-informaciyi

2. Нормативні документи системи ТЗІ Держспецзв’язку. URL: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi

3. Положення про метрологічну службу Адміністрації Державної служби спеціального зв'язку та захисту інформації України. URL: https://zakononline.com.ua/documents/show/83406___534619#n11

4. Пановик У. П. Стандартизація інтернету речей: сучасний стан та перспективи розвитку. *Поліграфія і видавнича справа*. 2023. № 1 (85). С. 51–64. URL: http://pvs.uad.lviv.ua/static/media/1-85/7.pdf

УДК 004.056.5:004.056.54:005.8(045)

ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УПРАВЛІННІ СКЛАДНИМИ ТЕХНІЧНИМИ ОБ'ЄКТАМИ

Пановик Уляна, Єсик Назарій, Богоніс Олександр
Українська академія друкарства,
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. Розглянуто ключові аспекти оптимізації стратегій управління інформаційною безпекою в умовах складних технічних об'єктів. Проаналізовані основні компоненти центру операцій інформаційної безпеки (SOC), зокрема, системи управління інцидентами, та їхній вплив на прийняття рішень у реальному часі. Зокрема, досліджуються функції та роль SIEM-системи і NTA-системи в підтримці ефективної роботи SOC.

Ключові слова: інформаційна безпека, управління ризиками, SOC, прийняття рішень, технічні об'єкти.

Abstract. The key aspects of optimizing information security management strategies in the conditions of complex technical objects are considered. The main components of an information security operations center (SOC), including incident management systems, and their impact on real-time decision-making are analyzed. In particular, the functions and role of the SIEM system and the NTA system in supporting the effective operation of the SOC are investigated.

Keywords: information security, risk management, SOC, decision-making, technical objects.

У сучасному технічному середовищі, де складні технічні об'єкти стають неодмінною частиною промислових та корпоративних систем, питання інформаційної безпеки набувають великого значення. Масштабні інфраструктури, такі як енергетичні системи, транспортні мережі та виробничі комплекси, потребують ефективного управління, щоб забезпечити надійність та захист інформації. З метою покращення цього процесу, важливим є розроблення систем підтримки прийняття рішень щодо інформаційної безпеки. Такі системи можуть забезпечити необхідний інструментарій для аналізу, моніторингу та ефективного управління ризиками, пов'язаними з інформаційною безпекою складних технічних об'єктів.

Перший крок у вирішенні цього завдання – це розуміння конкретних викликів, які виникають при управлінні інформаційною безпекою в складних технічних системах [1]. Серед таких викликів можуть бути ідентифікація потенційних загроз, оцінка вразливостей системи, планування заходів забезпечення безпеки та реагування на інциденти. Далі, розробка інтегрованих систем підтримки прийняття рішень може охоплювати застосування аналітичних методів та технологій для обробки великих обсягів даних, зокрема, застосування штучного інтелекту та машинного навчання. Це дає можливість не лише виявляти потенційні загрози, а й передбачати їхні можливі

виникнення, що полегшує прийняття рішень на ранніх стадіях [2]. Важливим компонентом системи підтримки прийняття рішень є також моніторинг та аналіз у реальному часі, що дає змогу оперативно реагувати на зміни в інформаційному середовищі та запобігати можливим інцидентам безпеки.

Для виявлення інцидентів на початкових етапах атак використовується центр моніторингу та реагування на інциденти інформаційної безпеки, відомий як *security operations center* (SOC). Основним завданням SOC є нагляд за активністю в IT-інфраструктурі, аналіз подій, виявлення загроз інформаційної безпеки та відповідь на них [3]. Виявлення потенційних загроз безпеці системи здійснюється під час збирання події з різних джерел, таких як ПК, сервери, бази даних, бізнес-системи та мережеве обладнання включно з мережевим трафіком. Для розв'язання цих завдань використовуються компоненти SOC, зокрема, системи класу *security information and event management* (SIEM), які автоматизують збір подій та виявлення інцидентів інформаційної безпеки.

SIEM-система діє як централізоване вікно для всіх подій від підключених джерел. Збір подій в SIEM-системі реалізується за допомогою спеціальних правил нормалізації, які дають можливість системі розпізнати, що отримується події з конкретного джерела, та структурувати дані за визначеними параметрами (час події, користувач, IP-адреса тощо). Це надає інформаційній безпеці можливість отримувати події в єдиному форматі, що зручно, як для ручного аналізу, так і для автоматизованого порівняння подій.

Зазвичай, SIEM-системи використовують бази даних для проведення аналізу поведінки користувачів та облікових записів, відомі як *user and entity behavior analytics* (UEBA). Цей аналіз ґрунтується на виявленні відхилень від середньостатистичних даних, зібраних упродовж тривалого періоду. Наприклад, якщо співробітник увійшов у систему вперше за пів року в ночі, це може свідчити про потенційний інцидент. SIEM-системи, як правило, використовують стандартні журнали інших систем, таких, як операційні системи, мережеве обладнання, антивірусні засоби, міжмережеві екрани, Active Directory, DNS та DHCP-сервери. Рівень деталізації, з яким фахівці SOC можуть проаналізувати події, залежить від налаштувань журналювання на цільовій системі. Для виявлення подій на кінцевих точках користувачів та серверах в IT-інфраструктурі може бути використаний інструмент класу *endpoint detection and response* (EDR). Цей інструмент не лише має вбудовані механізми журналювання, але також детально аналізує події на рівні операційної системи.

Важливим джерелом для виявлення інцидентів може бути мережевий трафік в IT-інфраструктурі. Для автоматизації збору та аналізу подій, що відбуваються в трафіку, використовуються інструменти класу *network traffic analysis* (NTA). NTA-система може функціонувати, як самостійний засіб із власними двигунами нормалізації та кореляції, а також слугувати джерелом даних щодо інцидентів інформаційної безпеки для SIEM-системи. Основна відмінність від звичайних систем виявлення мережевих атак (IDS) полягає в

тому, що NTA-система працює з великими обсягами трафіку. Це дає можливість виявляти повний цикл атак, а не обмежуватися окремою сигнатурою. Крім того, NTA-система зберігає копію трафіку для подальшого аналізу. На збереженій копії можна перевіряти нові індикатори компрометації (IOC). Додатково, збережений трафік сприяє проведенню докладного розслідування кіберінциденту та допомагає на основі аналізу виявляти невідомі загрози.

Також, для виявлення невідомих загроз, можна використовувати аналіз поведінки будь-якого програмного забезпечення, яке потрапило до IT-інфраструктури, незалежно від того, чи це знімний диск, Інтернет чи внутрішня мережа. Для цього аналізу використовуються інструменти класу *sandbox* (пісочниці). Пісочниця може вивчати поведінку об'єкта всередині спеціально створеного середовища та виносити рішення про те, наскільки об'єкт може бути небезпечним. Рекомендовано проводити перевірку всіх файлів всередині трафіку, якщо відправити потік файлів із трафіку від NTA до пісочниці. Знайдені рішення та індикатори файлів можна використовувати, як у NTA, так і в SIEM-системі. Коли не вистачає достатньої інформації, то тоді можуть бути використані засоби управління активами (AM) та управління вразливістю (VM). Такі системи можуть бути, наприклад, у ролі сканерів вразливостей, які за допомогою активного мережевого сканування допомагають складати списки активів в IT-інфраструктурі та фіксувати їх вразливості. Це дасть змогу належним чином оцінити загрози та інциденти з огляду на спроби злому, які зафіксовані у SIEM-системі, і визначити ступінь небезпеки цих спроб для конкретної атакованої системи.

У підсумку, підтримка прийняття рішень щодо інформаційної безпеки в управлінні складними технічними об'єктами є важливим напрямком розвитку в умовах зростаючих викликів у кіберпросторі. Впровадження інтегрованих та інтелектуальних систем допомагає підвищити рівень захисту інформації та забезпечити стабільність функціонування складних технічних об'єктів в умовах сучасного цифрового середовища.

Література

1. Пановик У. П. Системний підхід до управління ризиками інформаційної безпеки. *Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України*: Тези доп. IX Всеукр. заоч. науково-практ. конф., м. Київ, 2023 р. с. 125–126. URL: https://kztdop.ipf.npu.edu.ua/science-conference/conferenc-bgd.

2. Reeves A., Ashenden D. (2023). Understanding decision making in security operations centers: building the case for cyber deception technology. *Frontiers in Psychology*. *Vol. 14*. https://doi.org/10.3389/fpsyg.2023.1165705

3. Happa J., Agrafiotis I., Helmhout M., Bashford-Rogers T., Goldsmith M., Creese S. (2021). Assessing a decision support tool for SOC analysts. *Digital Threats Res. Pract.* 2, 1–35. https://dl.acm.org/doi/10.1145/3430753

УДК 004.056.5:004.738.5

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИСТРОЇВ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ АВТОМАТИЗАЦІЇ ВИРОБНИЧИХ ПРОЦЕСІВ

Пановик Уляна, Король Тетяна, Кутас Сергій
Українська академія друкарства,
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. Розглядається актуальне питання кібербезпеки для пристроїв у мережі Інтернету речей. Проведено аналіз загроз та викликів, що виникають у зв'язку з розширенням IoT, та досліджено засоби та стратегії для забезпечення захисту інформації для підвищення рівня безпеки та стійкості IoT-пристроїв у сучасному інтернет-середовищі. Дослідження спрямоване на вдосконалення заходів інформаційної безпеки та захисту конфіденційності в мережі Інтернету речей.

Ключові слова: пристрої Інтернету речей (IoT), загрози кібербезпеці, засоби захисту інформації.

Abstract. The topical issue of cybersecurity for devices on the Internet of Things network is considered. An analysis of the threats and challenges arising from the expansion of the IoT is carried out, and the means and strategies to ensure the protection of information to increase the level of security and resilience of IoT devices in today's Internet environment are explored. The study is aimed at improving information security and privacy protection measures on the Internet of Things network.

Keywords: Internet of Things (IoT) devices, cyber security threats, information protection tools.

Основними процесами в роботі систем Інтернету речей (IoT) є збір, передача й аналіз даних. Датчики, що встановлені на пристроях, реєструють інформацію про стан об'єкта або довкілля. Після цього отримані дані передаються на сервери або хмарні сервіси, де проводиться обробка й аналіз цих даних. Після аналізу генеруються відповідні команди, які надсилаються виконавчим пристроям або системам для виконання необхідних дій. Для передачі даних у системах IoT використовуються як дротові, так і бездротові мережі. Дротові мережі включають Ethernet, оптоволоконні кабелі та інші типи кабельних з'єднань, у той час, як бездротові мережі використовують технології, такі як Wi-Fi, Bluetooth, Zigbee, LoRaWAN, мобільні мережі (3G, 4G, 5G) й інші бездротові засоби передачі даних [1].

IoT значно впливає на виробничі процеси і промисловість загалом, зокрема на автоматизацію виробництва. За допомогою IoT-пристроїв, таких як роботи, сенсори та контролери, можна автоматизувати багато виробничих операцій, забезпечуючи високу точність, швидкість та ефективність. Окрім автоматизації, IoT допомагає впроваджувати системи обслуговування обладнання, завдяки збору та аналізу даних із датчиків. Це дає

змогу передбачити потребу в обслуговуванні або ремонті обладнання, запобігаючи збоям і зупинкам виробництва. IoT сприяє підвищенню продуктивності в промисловості, даючи можливість моніторити та оптимізувати роботу обладнання і персоналу. Це призводить до зменшення витрат на енергію, сировину та робочу силу. Застосування IoT відкриває також нові можливості для віддаленого моніторингу і управління виробничими процесами, що дає змогу операторам реагувати на зміни умов виробництва і уникати втрат часу та ресурсів.

Попри популярність та зручність IoT-пристроїв, вони мають свої недоліки. Особливо важливою є кібербезпека, оскільки кожен пристрій IoT може бути потенційною вразливою точкою входу в мережу та виробничих процесів. З розвитком технологій безпека IoT-пристроїв стає дедалі важливішою. Забезпечення безпеки пристроїв Інтернету речей (IoT) є важливою складовою сучасної мережі в організаціях[2]. ІТ-команди мають включити ці ризики у свої протоколи кібербезпеки і працювати над їх мінімізацією. Без належних практик щодо безпеки IoT, компанії можуть зіткнутися з новими кіберзагрозами, які надходять із кіберпростору. Наприклад, зловмисники, які спрямовані на розумні пристрої, можуть отримати доступ до критичних ресурсів компанії, подолавши вразливі розумні пристрої, які підключені до них. Це дає їм можливість збирати конфіденційні дані або влаштовувати систему виснажливих кібератак [3, 4].

Ризики, пов’язані з IoT, інколи легко прогледіти, якщо не використовувати відповідні інструменти. Іноді фахівці з інформаційної безпеки можуть недооцінювати важливість інвентаризації кінцевих точок, що може призвести до недооцінки потенційно вразливих пристроїв, які не отримують належної уваги. Найпоширенішими атаками на IoT є: DDoS-атаки, експлойти програмного забезпечення, атаки типу «людина посередник» (MITM-атаки), фізичне втручання, брутфорс-атаки та викрадення прошивки. Із цього випливає, що основні компоненти систем IoT вразливі до кібератак, і безпека має бути важливою на кожному етапі їхньої розробки та інтеграції. Для запобігання кібератакам на пристрої IoT і загальному зменшенню ризиків безпеки, компанії можуть застосовувати такі практики:

Управління поверхнею атаки. Планування заходів забезпечення безпеки IoT має включати створення карт, що охоплюють усі підключені пристрої для їхньої інвентаризації. Інформація про кількість пристроїв, виробників, серійні номери, версії обладнання та прошивки є важливою для команди безпеки, щоб керувати ризиками IoT.

Моніторинг, аналіз та звітність у режимі реального часу. Важливо, щоб компанії мали можливість постійно відстежувати стан безпеки IoT-пристроїв і реагувати на потенційні загрози в реальному часі. Використання програмних продуктів для інвентаризації та моніторингу підключених IoT-пристроїв допомагає відстежувати їхню активність і виявляти можливі аномалії та загрози.

Сегментація мережі є важливим кроком для запобігання доступу до всієї мережі організації, обмеження поверхні атаки та мінімізації можливих збитків. Сегментація мережі полягає в розділенні внутрішньої мережі на окремі підмережі. Ці сегменти можуть спілкуватися між собою, але вони зазвичай є незалежними та ізольованими. Цей підхід дає можливість зосереджувати увагу на критичних частинах мережі для посилення їх безпеки.

Створення надійних паролів для пристроїв IoT є також важливим заходом безпеки. Багато IoT-пристроїв постачаються зі слабкими попередньо встановленими паролями, які можуть бути легко підібрані. Під час реєстрації нового IoT-пристрою в мережі, рекомендується негайно змінити його попередньо встановлений пароль на складніший. Цей новий пароль має бути стійким до підбору, унікальним для кожного пристрою та відповідати політиці керування паролями вашої команди з безпеки ІТ.

Фізичний захист пристроїв на фізичному рівні має велике значення, оскільки доступність пристроїв ззовні може призвести до фізичних втручань зловмисників із метою несанкціонованого доступу або завантаження шкідливого програмного забезпечення. Тому варто забезпечити надійне місце дислокації пристроїв, щоб до них не було відкритого доступу.

Своєчасне оновлення прошивок є важливим кроком у забезпеченні безпеки IoT. Нові версії прошивок можуть містити виправлення вже відомих програмних вразливостей пристрою. Проте оновлення прошивок також повинно перевірятися на автентичність, оскільки зловмисники можуть намагатися під виглядом оновлень завантажити на пристрій шкідливе програмне забезпечення. Необхідно контролювати версійну актуальність та завжди використовувати останні безпечні версії прошивок.

Виконання цих заходів безпеки допоможе користуватися пристроями IoT безпечно в організації, максимізуючи їх користь та мінімізуючи можливі ризики. Проте важливо пам’ятати, що кіберзагрози постійно розвиваються, тому потрібно залишатися в курсі нових подій у кіберпросторі та регулярно оновлювати заходи безпеки, використовуючи передові рішення для моніторингу та аналізу атак.

Література

1. Internet of things (IoT). URL: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT#

2. Пановик У., Кутас С., Брич Т. Керування безпекою інтернету речей на основі індексу довіри. *Інформаційна безпека та інформаційні технології*: тези доп. IV Міжнар. науково-практ. конф. ІБІТ 2022, м. Львів, 30 листоп. 2022 р. Львів. С. 39–41. URL: https://sci.ldubgd.edu.ua/jspui/handle/123456789/11434.

3. Internet of Things: information security challenges and solutions. URL: https://www.researchgate.net/publication/326559393_Internet_of_Things_information_security_challenges_and_solutions.

4. Spiegelmock M. IoT Security Through Open Certification. URL: https://spiegelmock.com/2017/08/14/iot-security-through-open-certification/

УДК 004.77

ОСОБЛИВОСТІ ТЕХНОЛОГІЇ ЗАХИСТУ МЕРЕЖІ – CISCO ASA

Полотай Орест, Баденко Владислав, Балацька Валерія
Львівський державний університет безпеки життєдіяльності

Описано основні властивості ASA, яка використовується компанією Cisco Systems в серії міжмережевих екранів

Ключові слова: захист комп'ютерних мереж, міжмережевий екран, Cisco ASA

Describes the main properties of ASA, which is used by Cisco Systems in a series of firewalls.

Keywords: protection of computer networks, firewall, Cisco ASA

Виклики безпеки, з якими стикаються сучасні компанії, зводяться до того, щоб розглянути всі можливі рішення і вибрати правильну комбінацію для захисту комп'ютерно\ мережі. Сьогодні доступно багато технологій і відповідних інструментів безпеки. Складність впровадження мережевої безпеки полягає не у відсутності відповідної технології безпеки, а у виборі рішення, яке найкраще відповідає вимогам мережі та бізнесу, а також у мінімізації витрат на підтримку та обслуговування інструментів безпеки, пропонованих кожним постачальником. Серед великої кількості обладнання, яке призначене для організації захисту комп'ютерних мереж, особливої уваги заслуговують пристрої адаптивного захисту Cisco ASA Series (рис. 1).

Обладнання Cisco ASA Series являє собою прості у розгортанні рішення, що інтегрують сервіси міжмережевого екрану, системи запобігання вторгненням (IPS), VPN з підтримкою SSL та IPSec, безпеки уніфікованих комунікацій (передача голосових відеоданих) та безпеки контенту в гнучке сімейство модульних продуктів. Розроблені в якості основного компонента мережі Cisco, що самозахищається, пристрої Cisco ASA Series надають інтелектуальний захист від загроз і послуги безпечних комунікацій, які зупиняють поширення атак перш, ніж вони зможуть вплинути на цілісність бізнесу. Пристрої Cisco ASA Series призначені для захисту мереж усіх масштабів і дозволяють організаціям скоротити загальні витрати на розгортання та експлуатацію одночасно забезпечуючи комплексну багаторівневу безпеку.

Рисунок 1 – Пристрій захисту Cisco ASA Series

Серія ASA базується на потужних функціях безпеки, які можна знайти в сімействі продуктів Cisco, включаючи міжмережевий екран PIX 500, датчик IDS 4200 і концентратор VPN 3000 Серія Cisco ASA пропонує адаптивний захист від загроз і разом відомі як Adaptive Threat Defence. Вона включає в себе технології Anti-X, Application Security і Network Containment and Control для забезпечення комплексного і повного захисту критично важливих ресурсів підприємства від широкого спектру зловживань. Один пристрій з вбудованою підсистемою безпеки і кореляції подій забезпечує захист мережі від багатьох невідомих загроз (комп'ютерних черв'яків і антивірусів), шпигунських і рекламних програм, інструментів аналізу трафіку, виявлення хакерської активності і запобігання вторгненням, запобігання атакам типу "відмова в обслуговуванні" (DoS). Обладнання захисту ASA – забезпечує надійний захист корпоративних мереж за допомогою контролю стану з'єднань та демонструє високу продуктивність. Він пропонує широкі можливості захисту, повністю приховуючи архітектуру внутрішньої мережі від зовнішнього спостерігача та діє як “прикордонник” між корпоративною мережею та Інтернет, виконуючи функції контролю.

Пристрої захисту ASA мають такі особливості:

• Вбудована операційна система. Cisco ASA працює під керуванням вбудованої захищеної операційної системи реального часу, яка не залежить від проблем захисту UNIX або Windows. Операційна система ASA спеціально була посилена з погляду захисту від мережевих атак. Вона розроблялася з метою захисту.

• Алгоритм ASA (Adaptive Security Algorithm). Алгоритм ASA записує характеристики з'єднань, зберігаючи цю інформацію в таблиці і використовуючи її для перевірки вихідних і вхідних пакетів, щоб переконатися, що стан сеансу залишається таким самим, як і при відкритті з'єднання. Поки змін не виявляється, трафік пропускається без затримки. При виявленні якоїсь невідповідності пересилання даних припиняється.

Переваги алгоритму ASA:

• Жоден з пакетів, у яких інформація про з'єднання та стан не відповідає даним таблиці алгоритму ASA, не зможе пройти через пристрій захисту ASA.

• Дозволяються усі вихідні з'єднання та стани, крім тих, що спеціально заборонені вихідними списками доступу. Вихідним називаються з'єднання чи стан, у якому ініціатор чи клієнт має інтерфейс із вищим рівнем безпеки, ніж адресат чи сервер. Внутрішній інтерфейс має найвищий рівень безпеки, а зовнішній – найнижчий. Для додаткових інтерфейсів можуть визначатись рівні безпеки між рівнями внутрішнього та зовнішнього інтерфейсів.

• Вхідні з'єднання та стани забороняються, якщо вони спеціально не дозволені каналами. Вхідним називається з'єднання чи стан, у якому ініціатор чи клієнт має інтерфейс із нижчим рівнем безпеки, ніж адресат чи сервер. Кожна трансляція адрес дозволяє безліч винятків, що дозволяє дозволити доступ з будь-якої машини, з будь-якої мережі або з будь-якого хоста в мережі Інтернет до хоста, заданого трансляцією.

– Усі спроби обійти зазначені правила відкидаються, і серверу syslog надсилається відповідне повідомлення.
– Відкидаються всі пакети ICMP, крім тих, які спеціально дозволені командою conduit permit icmp або access-list.

Отже, для забезпечення ефективного захисту комп'ютерних мереж необхідно використовувати сучасні технології захисту, серед яких варто виділити обладнання захисту Cisco ASA.

Література

1. Полотай О.І., Тлумак О. Вибір обладнання Cisco для розгортання корпоративної VPN-мережі. 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. 64–66.

2. Міжмережевий екран: що це таке і для чого він потрібен (texnogid.biz.ua) Веб сайт Техногід. [Електронний ресурс]: – режим доступу: https://texnogid.biz.ua/wi-fi/bezpeka/mizhmerezhevyj-ekran.html

3. Балацька В.С., Полотай О.І., Ящук В.І. Вразливість комп'ютерної мережі як проблема закладів вищої освіти. Зб. тез доп. VI Міжнар. наук.-практ. конф. "Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи". (м. Львів, 04 листопада 2021 р.). Львів : ЛДУБЖД, 2021

УДК 004.77

ОСОБЛИВОСТІ МІЖМЕРЕЖЕВИХ ЕКРАНІВ CISCO PIX FIREWALL

Полотай Орест, Дубик Ірина
Львівський державний університет безпеки життєдіяльності,
Національний університет "Львівська політехніка"

Описано основні властивості та характеристики міжмережевих екранів компанії Cisco Systems.
Ключові слова: міжмережевий екран, Cisco

The main properties and characteristics of the Cisco Systems network screens are described.
Keywords: electronic course security, Cisco

Розвиток сучасних технологій призводить до того, що до мережного обміну даними виявляють все більше інтересу. Це стосується як приватних осіб, так і організацій. У зв'язку з цим виникає необхідність захищати конфіденційну інформацію, розробляючи для цього ефективні системи. Міжмережевий екран — одне з таких рішень, що застосовуються в подібних ситуаціях.

Одна з головних функцій мережевих екранів — захист від несанкціонованого доступу сторонніх осіб. Її організовують для окремих сегментів або хостів у мережі. Найчастіше проникнення третіх осіб пов'язані з уразливими у двох компонентах:

- програмне забезпечення, встановлене на ПК;
- мережеві протоколи, за якими легко дізнаватися відправника.

Поки працює міжмережевий екран, він порівнює характеристики трафіку, що проходить через той або інший пристрій. Шаблони вже відомого шкідливого коду використовуються для отримання максимального результату. Якщо щось не так, з'являється повідомлення «Заблокований вхідний трафік, перевірте налаштування мережевого екрану».

По суті, міжмережевий екран — це програмний або програмно-апаратний тип системи, що відповідає за контроль інформаційних потоків. Але і апаратний варіант теж має попит.

Одними з потужних представників ринку мережевого апаратного забезпечення, є американською компанією Cisco Systems. Серед міжмережевих екранів даної фірми, особливої уваги заслуговують міжмережеві екрани сімейства Cisco PIX.

Cisco PIX (Private Internet Exchange) — міжмережевий екран з перетворенням мережевих адрес (NAT).

Міжмережевий екран Cisco Secure Private Internet Exchange (PIX) Firewall реалізує захист корпоративних мереж на рівні, який раніше був не доступним і при цьому є простим у використанні. PIX Firewall приховує мережу від зовнішнього світу і таким чином забезпечує абсолютну безпеку внутрішньої мережі. Відмінність від звичайних proxy-серверів, які виконують окрему обробку кожного мережевого пакета з істотним завантаженням центрального процесора полягає в тому, що PIX Firewall використовує спеціальну операційну систему подібну Unix реального часу, яка забезпечує набагато вищу продуктивність. Головна перевага брандмауера PIX Firewall це спеціальна схема захисту. І ця схема базується на використанні алгоритму адаптивної безпеки (adaptive security algorithm - ASA). Цей алгоритм ефективно приховує адресу користувачів від зловмисників. Даний адаптивний алгоритм забезпечує безпеку на рівні з'єднання, використовуючи контроль інформації про адреси відправника і одержувача, послідовності нумераці пакетів TCP, номери портів і додаткових прапорцях TCP. Дана інформація зберігається в спеціальній таблиці і ці дані перевіряються на відповідність із записами всіх вхідних пакетів.

Крім підвищення продуктивності, застосування спеціалізованої вбудованої операційної системи реального часу також забезпечує підвищення рівня безпеки. На відміну від операційних систем сімейства UNIX, вихідний текст яких широко доступний, Cisco PIX – власна розробка компанії, створена спеціально для вирішення завдань забезпечення безпеки. Для підвищення надійності міжмережевий екран PIX Firewall передбачає можливість установки в подвійній конфігурації в режимі «гарячого резервування», за рахунок чого в мережі виключається наявність єдиної точки можливого збою. Якщо два PIX-екрани будуть працювати в паралельному режимі, і один з них вийде зі строю, то другий в прозорому режимі «підхопить» виконання всіх функцій забезпечення безпеки.

В даний час користувачам Firewall пропонуються наступні моделі апаратно-програмних міжмережевих екранів Cisco Secure PIX Firewall – PIX 501, 506E, 515E, 525 і 535. В таблиці 1 приведені порівняльні характеристики.

Таблиця 1

Порівняльні характеристики Cisco Secure PIX Firewall

	Pix 501	Pix 506E	Pix 515	Pix 525	Pix 535
Продуктивність, мбіт/с	60	100	190	330	1667
Максимальне число з'єднань	7500	25000	130000	180000	500000
Кількість одночасно підтримуваних сесій	19500	53000	176000	625000	1000000
Підтримувані фізичні інтерфейси	1*10/100	2*10/100	6*10/100	8*10/100	10*10/100

Підтримувані логічні інтерфейси VLAN 8o2.1q	0	0	8	10	24
Продуктивність VPN (Triple DES / AES-128), Мбіт/сек	3/4,5	16/30	135/130	145/135	425/495
Максимальне число VPN-тунелей	10	25	2000	2000	2000

Міжмережевий екран Cisco Secure PIX Firewall також дозволяє уникнути проблеми нестачі адрес при розширенні і зміні IP-мереж. Технологія трансляції мережевиї ажрес Network Address Translation (NAT) робить можливим використання в приватній мережі як існуючих адрес, так і резервних адресних просторів.

Отже, для забезпечення ефективного захист мережевих потоків даних необхідно використовувати сучасні технології, серед чких варто виділити продукцію компанії Cisco Systems.

Література

1. Полотай О.І., Тлумак О. Вибір обладнання Cisco для розгортання корпоративної VPN-мережі. 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. 64–66.

2. Міжмережевий екран: що це таке і для чого він потрібен (texnogid.biz.ua) Веб сайт Техногід. [Електронний ресурс]: – режим доступу: https://texnogid.biz.ua/wi-fi/bezpeka/mizhmerezhevyj-ekran.html

3. Балацька В.С., Полотай О.І., Ящук В.І. Вразливість комп’ютерної мережі як проблема закладів вищої освіти. Зб. тез доп. VI Міжнар. наук.-практ. конф. “Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи”. (м. Львів, 04 листопада 2021 р.). Львів : ЛДУБЖД, 2021

УДК 351: 657

ВНУТРІШНІЙ АУДИТ ЯК ІНСТРУМЕНТ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

Ружанський Олександр
Інститут державного управління та наукових досліджень з цивільного захисту

Анотація. Інформаційна безпека організації державного сектору є складовою інформаційної безпеки України, яка входить до складу національної безпеки України. Автором представлено визначення поняття інформаційної безпеки організації. Зазначено, що застосування засобів автоматизації процесів у сфері цивільного захисту значно підвищують якість роботи виконавців та терміни опрацювання інформації, проте недосконаліть системи захисту інформації може призвести до несанкціонованого втручання, витоку службової та конфіденційної інформації, втрати документів, їх доступності та цілісності інформації. За результатами дослідження встановлено, що якісний внутрішній аудит сприятиме посиленню кібербезпеки у системі ДСНС, а висновки та рекомендації надані за результатами ІТ аудиту допоможуть підрозділам ДСНС управляти ризиками щодо забезпечення якості інформаційних систем, прикладного програмного забезпечення та своєчасно реагувати на них, провести поглиблену регламентацію ІТ-процесів, усунути проблеми інформаційної системи та розробити шляхи їх вирішення, оптимізувати інвестиції в ІТ, відповідно до планів розвитку установ.

Ключові слова: аудит, внутрішній аудит, ризик, управління ризиками, система управління, цивільний захист, інформаційна безпека.

Abstract. The information security of the public sector organization is a component of the Ukraine's information security, which is part of the national security of Ukraine. The author presents the definition of the information security concept by organization. The use of means of processes automation in the sphere of civil protection significantly increases the quality of the work of executors and the terms of information processing, however, the imperfection of the information protection system can lead to unauthorized intervention, leakage of official and confidential information, loss of documents, their availability and integrity of information are noted in this article. According to the results of the study, it was established that a high-quality internal audit will contribute to the strengthening of cyber security in the system of the State Emergency Service, and the conclusions and recommendations provided based on the results of the IT audit will help the departments of the State Emergency Service to manage risks related to ensuring the quality of information systems and application software and to respond to them in a timely manner, to carry out in-depth regulation of IT processes, eliminate the problems of the information system and develop ways to solve them, optimize investments in IT, in accordance with the development plans of institutions.

Keywords: audit, internal audit, risk, risk management, management system, civil protection, information security.

Запорукою ефективного функціонування організації є її інформаційна безпека. *Інформаційна безпека організації* – прийняття рішень управлінськими ланками з повним доступом до достовірної та об'єктивної інформації, наявність в організації ефективної системи захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом та інші з інформацією, які можуть завдати шкоди та впливати на діяльність організації.

Інформаційна безпека організації державного сектору є складовою інформаційної безпеки України, яка входить до складу національної безпеки України. За останні роки було докладено чимало зусиль до становлення та розвитку національної системи кібербезпеки. Важливим етапом її інституалізації стало прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [1], який є правовим підґрунтям для створення національної системи кібербезпеки та виконання її основними суб'єктами завдань у сфері кібербезпеки. Сьогодні в системі ДСНС існує необхідність удосконалення комплексної системи захисту інформації на локальну мережу для захисту відкритої інформації, на сьогоднішній день не розроблено нормативний документ, який визначатиме перелік конфіденційної інформації.

Застосування засобів автоматизації процесів у сфері цивільного захисту значно підвищують якість роботи виконавців та терміни опрацювання інформації, проте недосконаліть системи захисту інформації може призвести до несанкціонованого втручання, витоку службової та конфіденційної інформації, втрати документів, їх доступності та цілісності інформації. Засоби автоматизації процесів, які використовуються у кадрових підрозділах ДСНС, в принципі здатні забезпечити надійність та захищеність інформації. Проте, наявність застарілої комп'ютерної техніки та наявність неліцензійного програмного забезпечення, не дозволяє забезпечити належний захист інформації при створенні документів, та їх цілісність, створює ризики щодо втрати інформації, її пошкодження чи викривлення, а відсутність автоматизації в процесах створення та обробки інформації призводить до уповільнення проходження документів та потребує значних затрат часу на здійснення окремих процесів.

У зв'язку з вищезазначеним необхідно вжити низку заходів у сфері кібербезпеки в системі ДСНС, а саме:провести докорінну реформу системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки в навчальних закладах ДСНС України; забезпечити збереження наявного кваліфікованого кадрового потенціалу суб'єктів кібербезпеки у сфері цивільного захисту; стимулювати дослідження і розробки у сфері кібербезпеки, зокрема захищеного електронного документообігу, з урахуванням появи нових кіберзагроз і викликів, створення інформаційних систем та платформ. Кібергігієна у сфері цивільного захисту, цифрові навички, кіберобіз-

наність фахівців в системі ДСНС щодо сучасних кіберзагроз та протидії ним мають стати невід'ємними елементами в процесі підготовки кадрів зазначеної сфери, адже саме професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення є тими невід'ємними елементами, що складають національну безпеку України вцілому. Саме такий підхід має стати основою для розроблення нормативно-правових актів у сфері кібербезпеки у сфері цивільного захисту, а також для обґрунтування розподілу необхідних кадрових ресурсів системи ДСНС.

Якісний внутрішній аудит сприятиме посиленню кібербезпеки у системі ДСНС, адже, при ІТ аудиту для отримання незалежної й об'єктивної оцінки ІТ системи установи аудиторською групою досліджуються впроваджені інформаційні технології та інформаційне управління; організація ІТ процесів і контролю; оцінка ІТ ризиків установи; стан інформаційної безпеки; відповідність системи управління інформаційною безпекою міжнародним стандартам і нормам, таким як ISO 27001, NIST, CIS тощо, а також регуляторним і законодавчим вимогам у сфері інформаційної безпеки і надаються відповідні рекомендації із покращення та удосконалення цих процесів. Підвищення ефективності управління в системі ДСНС із застосуванням інформаційних технологій є дуже актуальним, адже використання автоматизованих систем призводить до зростання якості, швидкості обробки та передачі інформації, потік якої постійно зростає. Проведення ІТ аудиту вимагає від аудитора спеціального досвіду у сфері інформаційних технологій та з питань забезпечення установи управлінською інформацією, знань щодо методів і прийомів внутрішнього аудиту, вміння надати оцінку ризиків, пов'язаних з ІТ. Адже, аудитори надають оцінку того, чи ІТ заходи контролю належно розроблені для запобігання чи виявлення ризиків (ІТ аудитор оцінює ефективність розроблених заходів контролю, та визначає яких заходів бракує або які запроваджені заходи контролю не досягають відповідної цілі контролю) та оцінку реалізації ІТ заходів контролю у певний часовий проміжок відповідно до структури (ІТ аудитор повинен зібрати, узагальнити і оформити у файл докази про різні моменти у визначеному часовому періоді, щоб бути помірковано упевненим у тому, що ІТ захід контролю функціонував ефективно протягом усього часового проміжку).

Висновки та рекомендації надані за результатами ІТ аудиту допоможуть підрозділам ДСНС управляти ризиками щодо забезпечення якості інформаційних систем, прикладного програмного забезпечення та своєчасно реагувати на них, провести поглиблену регламентацію ІТ-процесів, усунути проблеми інформаційної системи та розробити шляхи їх вирішення, оптимізувати інвестиції в ІТ, відповідно до планів розвитку установ.

Література

1. Про основні засади забезпечення кібербезпеки України / Закон України № 2163-VIII від 5 жовтня 2017 року / Відомості Верховної Ради (ВВР), 2017, № 45, ст.403.

УДК 004.77

ВРАХУВАННЯ ПРИНЦИПІВ КІБЕРБЕЗПЕКИ ПРИ РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Савостян В.В, Любчак В.О
Сумський державний університет, м.Суми

У доповіді проаналізовано сучасні виклики кібербезпеки та сформульовано рекомендації щодо створення захищеного програмного забезпечення, розглянуто ключові принципи безпеки на всіх етапах розробки ПЗ та новітні технології для протидії кіберзагрозам.

The report analyzes modern cybersecurity challenges and provides recommendations for developing secure software, reviews key security principles at all stages of software development, and explores cutting-edge technologies for combating cyberthreats.

Аналіз основних тенденцій розвитку кіберпростору показує появу багатьох викликів у сфері кібербезпеки як на глобальному, так і на національному рівнях. Розглядаючи принципи забезпечення кібербезпеки, варто виділити ключові рекомендації для розробки та впровадження програмного забезпечення. Дотримання цих принципів є важливим для всебічного забезпечення безпеки програмних продуктів.

Пріоритетним завданням є значне вдосконалення та посилення існуючих методів ідентифікації та аутентифікації користувачів, шляхом широкого запровадження сучасних багатофакторних моделей аутентифікації з використанням біометричних даних. Також критично важливого значення набуває забезпечення надійного криптографічного захисту та шифрування даних для гарантованого запобігання несанкціонованому доступу до конфіденційної інформації. В умовах зростання кількості кібератак необхідно зосередитися на інноваційних стратегіях і технологіях для ефективного протистояння новим викликам у галузі кібербезпеки для програмістів [1].

Наведемо кілька прикладів таких технологій та стратегій:

- Штучний інтелект та машинне навчання: Використання алгоритмів машинного навчання для виявлення аномальних патернів у мережевому трафіку та поведінці користувачів. Це дозволяє автоматично виявляти небезпечні дії та атаки.
- Блокчейн технології: Застосування технологій блокчейн для забезпечення невід'ємності даних та захисту від кібератак, спрямованих на модифікацію чи видалення інформації.
- Мультифакторна аутентифікація: Застосування не тільки пароля, а й інших елементів аутентифікації, таких як біометричні дані чи одноразові коди, для підвищення рівня безпеки доступу до систем.

– Системи моніторингу та виявлення інцидентів (SIEM): Використання інтегрованих систем, які аналізують та кореляціюють дані з різних джерел для виявлення невідповідностей та потенційних загроз.
– Багаторівневий захист: Застосування комплексу захисних заходів на різних рівнях, включаючи мережевий, додатковий та операційний рівні.

Аналіз поточного стану кібербезпеки у сфері розробки програмних продуктів виявляє низку гострих системних проблем та викликів. Критично важливим є регулярне здійснення комплексного оцінювання рівня захищеності інформаційних систем для своєчасного виявлення та нейтралізації можливих загроз. Забезпечення належного рівня кібербезпеки на всіх етапах життєвого циклу розробки програмних продуктів, свою чергу, є ключовою запорукою їхньої надійності та стійкості до загроз. Ще на початковому етапі визначення вимог до системи має проводитися надзвичайно ретельний аналіз можливих загроз та формулювання детальних специфікацій вимог щодо забезпечення її безпеки [2].

На наступному етапі проектування системи комплексний захист має бути закладений в її архітектуру, включаючи ретельно продумане надійне шифрування та мінімізацію потенційних ризиків. Реалізація системи обов'язково передбачає суворе застосування найкращих відомих практик безпечного програмування та ретельну перевірку програмного коду на наявність вразливостей.

На завершальному етапі тестування системи має обов'язково здійснюватися експертна оцінка її стійкості до найбільш небезпечних відомих кібератак для гарантування належного рівня захищеності.

Для забезпечення високого рівня кібербезпеки на всіх етапах життєвого циклу розробки програмних продуктів вирішальне значення має активне впровадження найсучасніших інноваційних технологій, таких як: глибинний статичний та динамічний аналіз програмного коду, масштабна автоматизація процесів тестування на проникнення та вразливості, технології DevSecOps, що передбачають повну інтеграцію заходів безпеки в усі процеси розробки, тестування та впровадження програмних рішень.

В свою чергу DevSecOps – це парадигма розробки програмного забезпечення, яка враховує аспекти безпеки на всіх етапах життєвого циклу розробки (SDLC). Вона поєднує DevOps (розробка і операції) з безпекою (Security), намагаючись вирішити проблеми безпеки на ранніх етапах розробки [3].

Основні аспекти DevSecOps включають:

– Автоматизація тестування на вразливості: DevSecOps передбачає використання інструментів автоматизованого тестування на вразливості для виявлення можливих проблем безпеки на ранніх етапах розробки.

– Інтеграція безпеки в CI/CD конвеєр: Безпека вбудовується в процес неперервної поставки (CI/CD), забезпечуючи швидке та безпечне внесення змін в продукт.
– Моніторинг та реагування на загрози в реальному часі: Використання систем моніторингу для виявлення погроз та автоматичної реакції на їх.
– Культура безпеки: Створення культури безпеки, де всі учасники розробки відповідають за безпеку продукту.
– Організаційні зміни: Перехід до DevSecOps часто потребує організаційних змін, включаючи спільну відповідальність за безпеку серед розробників, тестувальників і адміністраторів.

Отже, в умовах стрімких глобальних трансформацій та лавиноподібного наростання новітніх кіберзагроз, надзвичайно важливо забезпечити системне застосування сучасних підходів та комплексну імплементацію передових принципів кібербезпеки на всіх етапах та рівнях для створення стійкого захищеного програмного забезпечення.

Література

1. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions / Ö. Aslan et al. *Electronics*. 2023. Vol. 12, no. 6. P. 1333. URL: https://doi.org/10.3390/electronics12061333 (date of access: 20.11.2023).

2. Systematic literature review on security risks and its practices in secure software development / R. A. Khan et al. *IEEE access*. 2022. Vol. 10. P. 5456–5481. URL: https://doi.org/10.1109/access.2022.3140181 (date of access: 20.11.2023).

3. Introduction. *DevSecOps Docs*. URL: https://devsecopsdocs.com/docs/prologue/introduction/ (date of access: 20.11.2023).

UDC 004.77

METHODS OF CRYPTOGRAPHIC PROTECTION

Семчишин Андрій
Українська академія друкарства

In an era dominated by digital communication and information exchange, the paramount importance of securing sensitive data cannot be overstated. As technology continues to advance, so do the methods employed by malicious entities to compromise the confidentiality and integrity of information. In the realm of information security, cryptographic protection stands as a stalwart defense, providing a shield against unauthorized access and ensuring the sanctity of communication channels.

"Methods of Cryptographic Protection" delves into the intricate world of safeguarding data through the application of cryptographic techniques. This theme explores the diverse array of methods employed to encode, decode, and authenticate information, with the ultimate goal of fortifying the digital landscape against cyber threats. From classical encryption algorithms to cutting-edge cryptographic protocols, the journey through this theme unravels the layers of complexity involved in securing data and communications in an interconnected and data-driven society.

As we navigate an increasingly interconnected world, understanding and implementing robust cryptographic protection methods become imperative. This theme serves as a comprehensive guide, shedding light on the principles, algorithms, and strategies that underpin cryptographic defenses, empowering individuals and organizations to navigate the digital landscape with confidence and resilience.

The main problem addressed in the theme "Methods of Cryptographic Protection" revolves around the persistent challenge of securing sensitive information in the face of evolving cyber threats. As technology advances and communication becomes more digitized, the vulnerabilities in data transmission and storage become increasingly apparent. The overarching problem is the need to establish reliable and robust mechanisms to protect information from unauthorized access, interception, tampering, or any form of malicious exploitation.

Cryptographic protection aims to address this problem by employing mathematical algorithms and protocols to secure data, ensuring its confidentiality, integrity, and authenticity. However, the ongoing arms race between those seeking to protect information and those attempting to compromise it poses a continuous challenge. The development of more sophisticated attack techniques, the emergence of quantum computing threats, and the need for seamless integration with modern technologies are all facets of the overarching problem in cryptographic protection.

In essence, the main problem of this theme lies in striking a delicate balance between staying ahead of potential threats, adapting to emerging technologies, and maintaining the usability and efficiency of cryptographic methods in the relentless pursuit of safeguarding sensitive information in an ever-changing digital landscape.

The solution to the problem of securing sensitive information through cryptographic protection involves a multi-faceted approach that addresses various aspects of information security.

Here are the key components of the solution:

Continuous Research and Innovation:

Stay ahead of potential threats by fostering a culture of continuous research and innovation in cryptographic methods. This includes developing new encryption algorithms, cryptographic protocols, and security mechanisms to counter emerging risks.

Quantum-Resistant Cryptography:

Anticipate the potential threat posed by quantum computing by developing and implementing quantum-resistant cryptographic algorithms. This involves researching and adopting cryptographic methods that can withstand the computational power of quantum computers, ensuring long-term security.

Integration with Emerging Technologies:

Ensure seamless integration of cryptographic protection with emerging technologies such as the Internet of Things (IoT), artificial intelligence, and cloud computing. This integration should be designed to address the unique security challenges presented by these technologies while maintaining the efficiency and effectiveness of cryptographic measures.

User Education and Training:

Recognize the human factor in information security and invest in user education and training programs. This includes raising awareness about secure practices, promoting the use of strong passwords, and fostering a security-conscious culture within organizations and among individuals.

Regulatory Compliance:

Adhere to and enforce regulatory standards and compliance requirements related to information security. This ensures that organizations implement and maintain adequate cryptographic protection measures to safeguard sensitive data, taking into account legal and regulatory frameworks.

Collaboration and Information Sharing:

Foster collaboration and information sharing among industry stakeholders, researchers, and cybersecurity experts. This collaborative approach can help disseminate knowledge about emerging threats and effective countermeasures, creating a more resilient cybersecurity ecosystem.

Regular Security Audits and Assessments:

Conduct regular security audits and assessments to identify vulnerabilities and weaknesses in cryptographic implementations. This proactive approach allows organizations to address potential issues before they can be exploited by malicious actors.

By implementing these solutions collectively, organizations and individuals can enhance the effectiveness of cryptographic protection, mitigate risks, and navigate the evolving landscape of information security with greater confidence.

The key lies in a proactive and adaptive approach to staying ahead of potential threats while maintaining the usability and efficiency of cryptographic methods.

The theme of "Methods of Cryptographic Protection" underscores the critical importance of securing sensitive information in our digital age. As technology evolves, so do the methods employed by malicious actors, necessitating a robust and dynamic approach to cryptographic protection. Throughout our exploration of this theme, we've delved into the intricate world of encryption algorithms, cryptographic protocols, and security measures designed to fortify the confidentiality, integrity, and authenticity of data.

The persistent challenge lies in finding a delicate equilibrium between staying ahead of emerging threats and maintaining the usability of cryptographic methods. The continuous research and innovation in cryptographic techniques, coupled with the integration of quantum-resistant cryptography and adaptation to emerging technologies, form the foundation of a comprehensive solution. However, it is equally crucial to address the human element through education, regulatory compliance, and collaborative efforts to create a resilient cybersecurity ecosystem.

As organizations and individuals navigate the complexities of safeguarding information, regular security audits and assessments become essential tools for identifying vulnerabilities and reinforcing cryptographic implementations. The collective commitment to proactive measures, information sharing, and adherence to best practices is paramount in ensuring the efficacy of cryptographic protection.

In the face of an ever-evolving digital landscape, the journey through "Methods of Cryptographic Protection" reaffirms the significance of a holistic and adaptive approach to information security. By embracing innovation, collaboration, and a culture of vigilance, we can fortify our defenses, protect sensitive data, and foster a secure environment for communication and exchange in our interconnected world.

References

1. "Cryptography and Network Security: Principles and Practice" by William Stallings, 2008.
2. "Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier, 2014.
3. "Serious Cryptography: A Practical Introduction to Modern Encryption" by Jean-Philippe Aumasson, 2017.
4. "Handbook of Applied Cryptography" by Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, 2018.
5. "Understanding Cryptography: A Textbook for Students and Practitioners" by Christof Paar and Jan Pelzl, 2019.

УДК 004.056.5

ЗАСТОСУВАННЯ МЕТОДІВ OSINT В DARKNET

Селюкова Анна
Національний університет «Одеська політехніка»

Анотація. DarkNet розглядається як частина Інтернету, недоступна звичайним користувачам і часто використовувана для незаконних операцій. Автор пропонує програмний комплекс, який вирішує проблему пошуку та перевірки поштових адрес у DarkNet з метою подальшого ідентифікування користувача, що може слугувати інструментом в боротьбі з кібер-злочинністю. В роботі наведено загальний опис принципів роботи програмного комплексу та його можливостей, наведений приклад використання та окреслені перспективи подальшого розвитку.

Ключові слова: DarkNet, електронна пошта, Tor, пошук електронної пошти, інформаційна безпека, кібер-злочини.

Abstract. The DarkNet is considered a part of the Internet that is not accessible to ordinary users and is often used for illegal operations. The author offers a software complex that solves the problem of searching and checking postal addresses in the DarkNet for the purpose of further identifying the user, which can serve as a tool in the fight against cybercrime. The work provides a general description of the principles of the software complex and its capabilities, an example of its use, and outlined prospects for further development.

Keywords: DarkNet, e-mail, Tor, e-mail search, information security, cybercrime.

DarkNet є частиною Інтернету, яка недоступна для звичайних користувачів. Вона використовує спеціальні технології для приховування IP-адрес користувачів і сайтів, що робить її ідеальним середовищем для незаконної діяльності. Згідно з дослідженнями, більшість сайтів у DarkNet пропонують нелегальні товари і послуги. У 2014 році вчені з Люксембурзького університету виявили, що 44% англомовних адрес з 2618 проаналізованих у браузері Tor були пов'язані з торгівлею наркотиками, зброєю або підробленими товарами. Ще 31% адрес не могли бути ідентифіковані, але також могли бути пов'язані з незаконними операціями. [1] У 2016 році Мур і Рід оцінили 2723 відомі адреси Tor і виявили, що 57% цих сервісів були незаконними. [2] Ці дослідження показують, що DarkNet є значною проблемою для правоохоронних органів, які намагаються боротися зі злочинністю в Інтернеті.

Метою роботи є розробка програмного комплексу для пошуку та перевірки на існування адрес електронної пошти у мережі Darknet з подальшим використанням отриманих даних для ідентифікації особистості.

Зазвичай, поштова адреса є важливим елементом ідентифікації людини і цінним ресурсом для злочинців. Вони можуть використовувати її для одержання товарів і послуг, таких як наркотики, зброя або підроблені товари, або ж для зламу чужих поштових адрес (наприклад, використовуючи методи spear fishing) з ціллю отримання доступу до особистої інформації жертв. Запропонована розробка може стати ефективним інструментом в боротьбі з цими загрозами, наприклад, для виявлення поштових адрес, які були скомпрометовані, що допоможе користувачам захистити свою особисту інформацію. Крім того, програмний комплекс може бути використаний для виявлення незаконної діяльності, що може допомогти правоохоронним органам при веденні подальших досліджень.

Загальні принципи функціонування запропонованого програмного комплексу можна описати наступним чином. Для забезпечення програмі швидкого доступу до сервісу Tor використовується утиліта torify з комплекту Tor. Принцип її роботи полягають у тому, що з її допомогою можна прозоро зв'язати потрібний додаток і бібліотеку tsocks, яка містить необхідні для проксування конфігураційні налаштування. Програма завантажує вхідну веб-сторінку і видобуває з неї всі поштові адреси. Для цього програма використовує регулярні вирази для пошуку послідовностей символів, які відповідають формату поштової адреси. Програма реалізує функцію domen_check, яка перевіряє наявність MX-записів для домену електронної пошти. Встановлюється з'єднання з SMTP-сервером, надсилається запит HELO. Для перевірки існування конкретної скриньки використовується метод з бібліотеки smtplib – SMTP.rcpt(address).

Головна логіка програми описана в функції main. Для зручності користувачів програма включає функції save_emails_to_file і get_emails_from_file, які дозволяють зберігати і завантажувати адреси електронної пошти з файлів.

Для обробки аргументів командного рядка використовується бібліотека argparse, яка надає користувачу можливість вибору між двома режимами роботи: отримання адрес електронної пошти з веб-сторінок (--get_emails) та завантаження їх у файл або перевірка існування для списку адрес з файлу (--check_emails). Для знаходження адрес програма використовує requests, щоб отримати вміст веб-сторінки та виводить її заголовок.

Для демонстрації роботи програми була здійснена перевірка веб сторінок сайту Everest Ransomware Group, список скомпрометованих поштових адрес було збережено у файл під назвою ‘everest4.txt’. На рис. 1 можна побачити виконану перевірку поштових адрес. З відповідей можна зробити висновок, що сервери успішно відправляли привітальне повідомлення, відповідаючи на звернення, а також, що адресат, з яким ми намагалися зв’язатися, був визнаний як прийнятний для цього сервера.

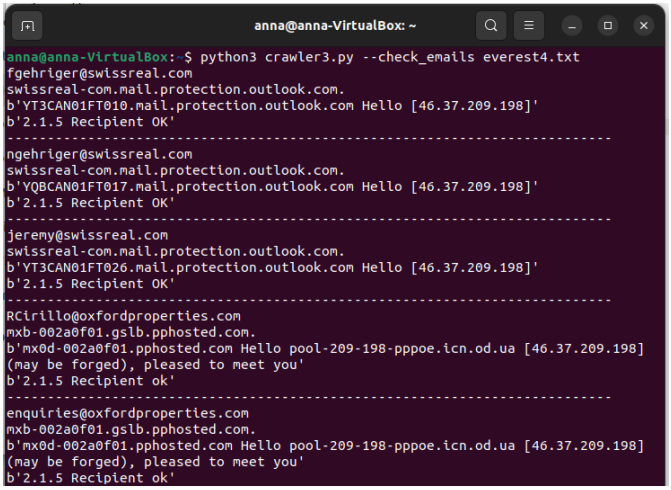


Рисунок 1 – Демонстрація роботи розробленого програмного комплексу

Переваги створеної програми проявляються у тому, що вона проста у використанні, що робить її доступною для користувачів з різним рівнем технічних знань. Також вона є достатньо надійною, що забезпечується декількома перевірками пошти, що, у свою чергу, забезпечує високу якість результатів пошуку, і швидкою, що дозволяє знаходити та перевіряти поштові адреси за відносно невеликий проміжок часу.

Загалом, програма є важливим кроком у вирішенні завдань, пов'язаних із збором та обробкою інформації з веб-сторінок і перевіркою доменів електронної пошти. Подальші дослідження та вдосконалення можуть розширити область її застосування. Планується розробити можливість підключатися до DarkNet через Tor без використання сторонньої утиліти, а через налаштування зроблені у самій програмі. Також може бути впроваджено лінгвістичну модель для аналізу тексту на веб сторінках для виявлення постів написаних одним автором.

Література

1. Biryukov, A., Pustogarov, I., Thill, F., & Weinmann, R. (2014). Content and popularity analysis of Tor hidden services. 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops. URL:https://doi.org/10.1109/icdcsw.2014.20

2. Moore, D., & Rid, T. (2016). Cryptopolitik and the darknet. Survival, 58(1), 7-38. URL:https://doi.org/10.1080/00396338.2016.1142085.

УДК 35:004.05

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Терент'єва Анна
Інститут державного управління та наукових досліджень з цивільного захисту

Для ефективного функціонування системи запобігання та реагування на надзвичайні ситуації потрібна своєчасна, безперервна, повна та достовірна інформація, без якої важко оцінити обстановку, можливості сил та засобів служб, призначених для запобігання та ліквідації їх наслідків, а також спроможність координувати спільні дії.

Базовим ресурсом для здійснення управлінської діяльності, зокрема опрацювання управлінських рішень, є адекватна інформація про надзвичайну ситуацію, отримання якої можливе за умов реалізації заходів, спрямованих на захист цієї інформації і систем обробки та передачі.

Наразі можна стверджувати про подальше удосконалення заходів інформаційної безпеки при супроводі прийняття управлінських рішень у сфері цивільного захисту, а також наголосити на нагальній потребі використання сучасних засобів комп'ютерної техніки та інформаційно-комунікаційних мереж для задоволення попиту на своєчасну та адекватну інформацію.

Ключові слова: управління, надзвичайна ситуація, інформація, інформаційна безпека, управлінське рішення.

The effective functioning of the system of prevention and response to emergencies requires timely, continuous, complete and reliable information, without which it is difficult to assess the situation, capabilities of forces and means of services designed to prevent and eliminate their consequences, as well as to coordinate joint actions.

The basic resource for the implementation of management activities, in particular the development of management decisions, is adequate information about an emergency, which can be obtained under the conditions of the implementation of measures aimed at protecting this information and processing and transmission systems.

Currently, it is possible to assert the further improvement of information security measures in support of management decision-making in the field of civil protection, as well as to note the urgent need to use modern computer equipment and information and communication networks to meet the demand for timely and adequate information.

Key words: management, emergency, information, information security, management decision.

За своєю природою надзвичайна ситуація як об'єктивне явище має в цілому невисокий ступінь передбачуваності за умови спонтанності прояву та складності прогнозування таких подій, зокрема стихійних лих. Тоді як з інформаційної точки зору за цих умов до моменту отримання інформації, достат-

ньої для опрацювання ефективних дій у відповідь, утворюється дефіцит часу для їх реалізації, що є управлінським парадоксом, тобто при очікуванні отримання достовірної і достатньої для прийняття рішень інформації, система реагування не спроможна врахувати непередбачуваних змін обстановки, а маючи невизначену інформацію, не може вживати адекватних заходів щодо реагування власне на надзвичайну ситуацію. Також за цих умов негативні впливи на об'єкти інформаційної безпеки можуть призвести до серйозних збитків життєво важливим інтересам та завдати значних соціально-економічних втрат державі, суспільству, репутації ДСНС України і його структурам, та окремим громадянам [1]. Саме тому управління інформаційною безпекою в умовах надзвичайних ситуацій є проявом соціального регулювання, в тому числі правового, а також політичної діяльності і організаційних заходів з протидії загрозам національним інтересам в інформаційній сфері.

Дослідники [2] наголошують, що наразі для інформаційної безпеки України базовими існуючими та ймовірними загрозами в сфері цивільного захисту визначено приховування, перекручення, несвоєчасне інформування населення про надзвичайні ситуації; недостатні спроможності інформаційно-телекомунікаційних систем щодо збирання, обробки та передачі інформації за цих умов; недостатню цифровізацію органів державної влади і місцевого самоврядування, що ускладнює моніторинг стану потенційно небезпечних об'єктів і територій, прогнозування й реагування на надзвичайні ситуації.

На нашу думку, забезпечення інформаційної безпеки в умовах надзвичайних ситуацій можна визначити як гарантування безпеки інформаційних систем для підтримки прийняття управлінських рішень щодо ліквідації їх наслідків, а також забезпечення безпеки процесу збору і обробки інформації, моніторингу виникнення надзвичайних ситуацій з використанням сучасних геоінформаційних технологій та імітаційного моделювання.

При ліквідації наслідків надзвичайної ситуації саме приховування, затримка надходження, спотворення і руйнування оперативної інформації, несанкціонований доступ до неї окремих осіб або груп осіб можуть привести як до людських жертв, так і до виникнення різного роду складнощів, пов'язаних з особливостями інформаційного впливу в екстремальних умовах: до неконтрольованого переміщення великих мас людей, що знаходяться в стані значного психоемоційного збудження; до швидкого виникнення і розповсюдження серед них паніки і заворушень на основі чуток, неправдивої або недостовірної інформації.

Погоджуємось із думкою авторки щодо того, що «… одним із пріоритетних напрямів безпекової політики України повинно стати підвищення безпеки та стійкості цивільного захисту по відношенню до усього спектру загроз і ризиків, оскільки саме критична інфраструктура забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та благополуччя, а також належний рівень національної безпеки» [3].

Таким чином, управління інформаційною безпекою в умовах надзвичайних ситуацій можна визначити як організацію, координацію і контроль операційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки з диференціацією окремих її елементів (об'єктів, суб'єктів, основних характеристик, рівнів інформаційної безпеки та переліку загроз). Констатуємо, що інформація у сфері захисту населення й територій від надзвичайних ситуацій техногенного та природного характеру, діяльність центральних та місцевих органів виконавчої влади, виконавчих органів рад у цій сфері є гласною і відкритою, якщо інше не передбачено законом. Зважаючи на вище викладене забезпечення розвитку спроможностей державних органів із забезпечення сталого функціонування до, під час та після настання надзвичайної (кризової) ситуації як елементу системи забезпечення національної стійкості тісно пов'язане з розвитком кращих практик управління інформаційною безпекою.

Література

1. Барило О. Г. Інформаційно-аналітичне забезпечення системи управління цивільного захисту держави. *Актуальні проблеми державного управління*. Зб. наук. пр. Одеса : ОРІДУ НАДУ. 2018. Вип. 1 (73). С. 45–50.

2. Волянський П.Б., Гур'єв С.О., Соловйов О.С., Терент'єва А.В. Кризовий менеджмент і принципи управління ризиками в процесі ліквідації надзвичайних ситуацій : монографія. К.: Парлам. вид-во, 2021. 432 с.

3. Усик С. Дослідження правового механізму забезпечення інформаційної безпеки в умовах надзвичайних ситуацій. *Науковий вісник: Державне управління*. 2021, № 4(6). С. 266-280.

УДК 004.056.5:005

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА СИСТЕМИ СТРАТЕГІЧНОГО УПРАВЛІННЯ ГОТЕЛЬНОГО ПІДПРИЄМСТВА

Усманова Маліка, Ящук Валентина, Фединець Наталія
Львівський торговельно-економічний університет, Львів, Україна,
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи забезпечення інформаційної безпеки як складової системи стратегічного управління готельного підприємства. Визначено сучасні підходи до проектування системи стратегічного управління готельного підприємства. Наведено методичні підходи до формування концепції забезпечення інформаційної безпеки. Запропоновано етапи вирішення науково-практичної проблеми, пов'язаної з підвищенням рівня інформаційної безпеки готельних підприємств.

Ключові слова: інформаційна безпека, системи стратегічного управління, готельне підприємство.

The theoretical, scientific-methodical and organizational-functional foundations of ensuring information security as a component of the strategic management system of a hotel enterprise are considered. Modern approaches to the design of the strategic management system of the hotel enterprise have been determined. Methodical approaches to the formation of the concept of ensuring information security are given. The stages of solving the scientific and practical problem related to increasing the level of information security of hotel enterprises are proposed.

Keywords: information security, strategic management systems, hotel enterprise.

Сьогодні спостерігається суттєве зростання ролі інформації в діяльності готельного підприємства. Інформація є одним з основних ресурсів готельного підприємства, що забезпечує його ефективне функціонування. Вона використовується для управління підприємством, надання послуг клієнтам, здійснення маркетингової діяльності тощо. Зростання ролі інформації в діяльності готельного підприємства вимагає підвищеної уваги до її безпеки. В сучасних умовах існує широкий спектр загроз інформаційній безпеці готельного підприємства, таких як хакерські атаки, розкрадання інформації, кібертероризм тощо. Ці загрози можуть призвести до серйозних фінансових збитків, порушення діяльності підприємства та навіть до його закриття. Готельні підприємства все частіше усвідомлюють важливість захисту інформації та впроваджують системи інформаційної безпеки. Це дозволяє їм підвищити рівень інформаційної безпеки, мінімізувати ризики та забезпечити безперебійну роботу підприємства. Дослідження актуальної теми "Інформаційна безпека як складова системи

стратегічного управління готельного підприємства" має важливе значення для забезпечення ефективного функціонування готельного підприємства та підвищення його конкурентоспроможності. Основні інформаційні загрози наведено на рис. 1.

Інформаційна безпека готелю є одним із найважливіших аспектів безпеки підприємства готельного бізнесу. Будь-яка протиправна дія проти інтересів готелю починається з отримання інформації про нього. Інформаційні системи готелю містять конфіденційні дані клієнтів і співробітників, а також інші важливі відомості. Порушення інформаційної безпеки може призвести до збоїв у роботі систем управління, розголошення комерційної таємниці та порушення достовірності фінансової документації.

Рисунок 1 – Основні групи інформаційних загроз готельних підприємств

Кіберзлочинність є однією з найактуальніших загроз для інформаційної безпеки готельних підприємств. Ця категорія злочинів включає в себе порушення чужих прав та інтересів у автоматизованих системах обробки даних. Готельний бізнес є особливо вразливим до кіберзлочинності, оскільки він має справу з конфіденційною інформацією гостей, зокрема даними банківських карток. Інформаційні системи готелей обробляють такі дані, як поштові адреси, номери контактних телефонів, адреси електронної пошти та дані кредитних і дебетових карт. Ця інформація може бути використана кіберзлочинцями для крадіжки особистих даних гостей, фінансових махінацій або навіть для організації кібератак на інші підприємства.

За даними досліджень, на готельний сектор припадає близько 15% від загального числа випадків витоку даних [1]. Це означає, що готелі є однією з найбільших цілей для кіберзлочинців. Щоб захиститися від кіберзлочинності, готелі повинні вжити заходів для підвищення рівня інформаційної безпеки. До таких заходів належать: впровадження сучасних систем

безпеки, які забезпечують захист від кібератак; підвищення обізнаності співробітників про кібербезпеку; впровадження політики конфіденційності, яка визначає правила обробки та захисту конфіденційної інформації. Готелі, які вживають заходи для підвищення рівня інформаційної безпеки, можуть мінімізувати ризик витоку даних та захистити своїх гостей та співробітників від кіберзлочинності.

Отже, для забезпечення інформаційної безпеки як складової системи стратегічного управління в готельних підприємствах потрібно [2] аналізувати й узагальнювати потенційні загрози та причини порушень; розробляти методики оцінки інформаційних ризиків; проводити інформаційні обстеження ресурсів підприємства; розробляти політику та концепції інформаційної безпеки; розробляти корпоративний стандарт забезпечення інформаційної безпеки готелю; частину інформації віднести до категорії обмеженого доступу (службова таємниця); стежити за експлуатацією технічних заходів захисту інформації.

З метою підвищення рівня інформаційної безпеки підприємств готельного бізнесу, необхідно своєчасно проводити аудит і контроль функціонування системи інформаційної безпеки; розробити механізм управління безпекою підприємства на засадах контролінгу; аналізувати загрози внутрішнього та зовнішнього середовища. Результати дослідження можуть бути використані для розроблення стратегії інформаційної безпеки готельного підприємства; впровадження заходів щодо підвищення рівня інформаційної безпеки готельного підприємства; підвищення кваліфікації працівників готельного підприємства з питань інформаційної безпеки.

Література

1. Інноваційні технології у готельному господарстві : навч. посіб. / Н. М. Влащенко ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2023. – 150 с.

2. Ящук В.І. Алгоритм проектування системи стратегічного управління готельно-ресторанним підприємством // В.І. Ящук , Степанюк К.А./ «Світ економічної науки. Випуск 5» : матеріали міжнародної науково-практичної інтернет-конференції економічного спрямування (м. Тернопіль, 26 червня 2018 року). – Тернопіль. – 2018. – 98 с. (С.41-45).

УДК 004.056.5:37.018.43

ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ДЛЯ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

Федина Богдана, Пановик Роман
Українська академія друкарства
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. Досліджуються сучасні засоби та стратегії для забезпечення конфіденційності, цілісності та доступності електронних документів. Аналізуються вимоги до захисту інформації, що зберігається та обробляється в системах документообігу. Розглядаються технологічні та організаційні аспекти впровадження засобів захисту для забезпечення стійкості інформаційних систем в умовах сучасного електронного середовища для закладів вищої освіти.

Ключові слова: захист інформації, системи електронного документообігу, стратегія безпеки.

Abstract. Explore modern tools and strategies for ensuring the confidentiality, integrity, and availability of electronic documents. The requirements for the protection of information stored and processed in document management systems are analyzed. The article examines the technological and organizational aspects of the implementation of protection measures to ensure the stability of information systems in the conditions of the modern electronic environment for institutions of higher education.

Keywords: information protection, electronic document management systems, security strategy.

Електронний документообіг описує сукупність дій, які включають зберігання, передачу, відправлення, створення, оброблення, одержання, використання та ліквідацію електронних документів у комп'ютерних мережах. Під управлінням електронним документообігом розуміється організація «руху документів» між підрозділами організації або підприємства, а також між окремими користувачами чи групами користувачів. У цьому контексті «рух документів» не вказує на їхнє фізичне переміщення, а на передачу прав на їх використання з повідомленням конкретних користувачів та контролем за їхнім використанням. Отже, документообіг означає створення інформаційної бази документів на різних носіях для використання управлінським апаратом під час виконання їхніх функцій [1].

Заклади вищої освіти (ЗВО) варто розглядати як великі організації, які є територіально розподіленою структурою з власними адміністративними системами життєзабезпечення і працюють на засадах децентралізованого управління. Тому інформаційна система закладу вищої освіти має бути корпоративною системою управління, яка інтегрує всі основні ділові процеси організації в комп'ютерні технології, має можливість взаємодіяти з іншими системами та складається з підсистем, що покращують її функціональність [2].

Автоматизація електронного документообігу в закладах вищої освіти дає можливість: зареєструвати документ у системі; паралельно виконувати різні операції для скорочення часу обробки документів та підвищення оперативності; забезпечувати неперервний рух документа; централізовано зберігати документи в єдиній базі; запобігати дублюванню документів; забезпечувати ефективний пошук у базі документів; здійснювати контроль за статусами, атрибутами та датами документів для поетапного їхнього оброблення; покращувати процедури підготовки, подачі/доставлення, обліку та зберігання документів; застосовувати єдиний шаблон документів для однорідності; прискорювати процес погодження проектів.

Застосування електронного документообігу в закладах вищої освіти не є складним процесом і не вимагає від користувачів глибоких знань у програмуванні або складних технічних навичок. Проте під час впровадження систем електронного документообігу у ЗВО виникають певні труднощі. Важливо пам'ятати про безпеку системи. Традиційний підхід до забезпечення безпеки інформації полягає в аналізі можливих загроз і встановленні відповідних механізмів захисту. Основні загрози безпеки системи включають:

- Загроза цілісності інформації: це може бути пошкодження, знищення або спотворення інформації, і ця загроза може бути, як ненавмисною, у разі збоїв, так і зловмисною.
- Загроза конфіденційності: охоплює порушення конфіденційності, такі як крадіжка, перехоплення інформації, зміна маршрутів передачі та інше.
- Загроза працездатності системи: це загроза, яка може призвести до порушення або припинення роботи системи, включаючи навмисні атаки, помилки користувачів, а також збої в обладнанні та програмному забезпеченні.
- Загроза доступності: ця загроза впливає на можливість користувачів отримувати доступ до необхідної інформації в прийнятний час.

Забезпечення безпеки в системі електронного документообігу важливо для забезпечення надійності й конфіденційності даних. Захист від зазначених загроз є важливою складовою будь-якої системи електронного документообігу. Для забезпечення безпеки інформації з обмеженим доступом, яка підпадає під вимоги закону, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах важливо вживати такі заходи: обмеження фізичного доступу до об'єктів системи документообігу; розмежування прав доступу до файлів і папок; підтвердження авторства електронного документа; контроль цілісності та конфіденційності електронного документа; забезпечення надійності функціонування технічних засобів; забезпечення резервування каналів зв'язку; резервне дублювання інформації; захист від вірусів; захист від «злому» мереж.

Особливу увагу варто приділити методам ідентифікації та автентифікації користувачів у комп'ютерних системах. Парольна ідентифікація є поширеною, простою для реалізації, але вимагає сильних паролів, щоб

уникнути підбору. Апаратний (електронний) метод ідентифікації використовує різноманітні пристрої, такі як карти і токени, і забезпечує високий рівень надійності, але може вимагати додаткового захисту від крадіжок або втрати цих пристроїв. Забезпечення безпеки ідентифікації та автентифікації користувачів є важливою складовою системи захисту електронного документообігу й допомагає запобігти несанкціонованому доступу до конфіденційної інформації [3].

Для організації захисту інформації в системі електронного документообігу важливо приділити особливу увагу двом аспектам: забезпеченню доступності публічної інформації та блокуванню несанкціонованого доступу. Однак основною проблемою під час організації захисту системи електронного документообігу є не технічні засоби, а лояльність користувачів. Коли документ потрапляє до користувача, конфіденційність цього документа вже порушена, і користувач може знайти різні способи копіювання інформації, від збереження на зовнішній носій до фотографування. Протоколювання дій користувачів є важливим елементом захисту електронного документообігу. Це дає можливість відстежувати всі неправомірні дії та знайти винуватця, а під час оперативного втручання, навіть, зупинити спроби неправомірних дій.

Підхід до захисту електронного документообігу має бути комплексним і охоплювати не лише захист документів та керування доступом до них, але також захист апаратного забезпечення системи, мережевого середовища, каналів передачі даних та інших аспектів. Крім того, важливо правильно оцінити можливі загрози та ризики для системи електронного документообігу і визначити можливі втрати від цих загроз.

Урахування організаційних заходів відіграє важливу роль у системі захисту на всіх рівнях. Необхідно впроваджувати елементарні та ефективні засоби, такі як системи паролів із розмежованим рівнем доступу, для забезпечення базового рівня захисту.

Література

1. Про електронні документи та електронний документообіг. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

2. Засторожнікова І.В. Електронний документообіг у сфері освіти. Державне управління та місцеве самоврядування. Дніпро, 2020. 3 (46). ст. 100-105. URL: https://journals.politehnica.dp.ua/index.php/public/article/view/162/141

3. Panovyk U., Sharadze A. The growth of cloud computing in the educational process under today's conditions. *Інформаційна безпека та інформаційні технології*: тези доповідей IV Міжнародної науково-практичної конференції ІБІТ 2022, Львів, 2022. URL: https://sci.ldubgd.edu.ua/jspui/handle/123456789/11434.

УДК 005.44:339.924

ОБҐРУНТУВАННЯ ВЗАЄМОЗВ'ЯЗКУ ПРОЦЕСІВ ГЛОБАЛІЗАЦІЇ ТА ДИВЕРСИФІКАЦІЇ НА ЕКСПОРТНИХ РИНКАХ

Шишлевський Михайло
Академія праці, соціальних відносин і туризму (Київ, Україна)

Анотація. Обґрунтовано основні проблеми забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках. Запропоновано напрями забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках, які полягають у поєднанні таких складових: наука і технологія, капіталовкладення, інфраструктура та інформація.

Ключові слова: диверсифікація, глобалізація, експорт, експортні ринки, конкурентоспроможність.

Abstract. Described the main problems of ensuring the effectiveness of globalization and diversification in export markets. Proposed directions for ensuring the effectiveness of globalization and diversification in export markets, which consist in a combination of separate components: science and technology, capital investment, infrastructure and information.

Key words: diversification, globalization, export, export markets, competitiveness.

Діджиталізація економіки стає ключовим фактором в умовах сучасних глобалізаційних та економічних викликів. Важливо розглядати діджиталізацію як стратегічний інструмент забезпечення ефективності, взаємодії процесів глобалізації та диверсифікації на експортних ринках [5; 6].

Сучасні умови господарювання супроводжуються кардинальними змінами в глобалізаційних процесах, що виникли в період всесвітньої пандемії та отримали продовження у зв'язку із війною, що розв'язала РФ.

Окреслені процеси зумовлюють необхідність перегляду ключових аспектів функціонування з урахуванням мінливих умов сьогодення та висувають на перший план питання забезпечення ефективного взаємозв'язку процесів глобалізації та диверсифікації на експортних ринках. Таке зауваження ґрунтується на тому, що саме оптимальний взаємозв'язок глобалізаційних та диверсифікаційних процесів здатний забезпечити ефективність експорту країни вцілому та окремих господарюючих суб'єктів зокрема [2]. До основних проблем забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках належать (рис. 1).

Процес забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках має бути спрямованим на:

1) побудову ефективної системи протидії ризикам зниження конкурентоспроможності диверсифікованих підприємств;

2) розробку механізму виявлення та ефективного використання конкурентних переваг диверсифікованих підприємств в умовах глобалізації експортних ринків;

3) обґрунтування напрямів забезпечення ефективності управлінських рішень та забезпечення їх узгодження із проявом негативних і позитивних чинників конкуренції на експортному ринку [3].

Стратегія забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках повинна полягати не тільки в збільшенні обсягів експорту, а й у створенні довгострокових конкурентних переваг та стабільному розширенні позицій диверсифікованих підприємств в умовах глобалізації світових ринків [1].

Україна має шанси для поліпшення своїх позицій на світовому ринку за умови забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках. Досягнення цього можливе завдяки проведення відповідної експортно орієнтованої політики, підґрунтям якої виступає забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках.

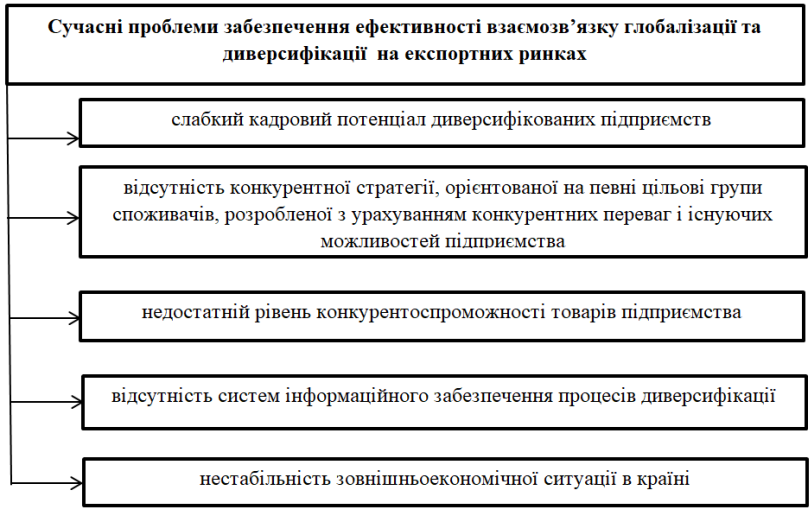


Рисунок 1 – Сучасні проблеми забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках
Укладено особисто автором.

У даному контексті можна запропонувати такі напрями забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках:

1. *Наука і технологія.* Україна має значний науково-технічний потенціал. Проте існує необхідність в розробці й удосконаленні шляхів його ефективного використання в процесі виходу на зовнішні ринки в якості експортера.

2. *Капіталовкладення,* підґрунтям яких повинні виступати іноземні інвестиції. Так, процесу забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках перешкоджає існуюча податкова система України як головний фактор, що заважає залученню іноземних інвестицій [4].

3. *Інфраструктура та інформація.* На сьогодні рівень розвитку цих двох факторів в Україні недостатній. Експортери мають низький рівень кваліфікації та інформативності про реальну ситуацію на міжнародних ринках, яка часто змінюється під впливом глобалізаційних чинників. Як наслідок виникають певні трудності при здійсненні експортних операцій, особливо в умовах диверсифікації, коли особливе значення має оперативна інформація

Крім того, ефективному формуванню стратегії забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках заважає недостатній розвиток інфраструктури. Ця проблема є актуальною, оскільки географічне положення України робить фактор інфраструктури вирішальним при визначенні експортного потенціалу кожного окремого суб'єкта зовнішньоекономічної діяльності та України в цілому. Крім того зараз ця проблема набула максимальної актуальності внаслідок руйнування логістичних шляхів російським агресором.

Враховуючи всі наведені фактори, методика розробки стратегії забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках повинна складатися з таких етапів: *перший* – аналіз ситуації, в якій знаходиться підприємство (можливості галузі, діяльність конкурентів, їх технології, стан експортних ринків, які обслуговуються; *другий* – аналіз внутрішнього стану компанії у співставленні з становищем справ у всій галузі та процес диверсифікації. На цій основі розробляється можлива стратегія розвитку кожного окремого підприємства.

Таким чином, стратегія забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках повинна розрахуватися таким чином, щоб її продукція зберігала високі конкурентні якості і технічну новизну протягом довгого часу. Такі компанії зберігають лідерство у світовому виробництві. Наукова новизна даного дослідження полягає в обґрунтуванні напрямів забезпечення ефективності взаємозв'язку глобалізації та диверсифікації на експортних ринках. При цьому в якості подальших досліджень доцільно вказати необхідність розробки шляхів виходу диверсифікованих підприємств на зовнішні ринки.

Література

1. Експортна стратегія України. Дорожня карта стратегічного розвитку торгівлі 2017–2021: Міністерство розвитку економіки, торгівлі та сільського господарства України. URL: https://me.gov.ua/Documents/Detail?lang=ukUA&id=e6ab10fa-0ad9-4fe4-b8be-32f570693b64&title=EksportnaStrategiiaUkrainiDorozhniaKartaStrategichnogoRozvitkuTorgivli2017-2021

2. Міжнародні відносини та зовнішня політика України: підручник / Ю. В. Пунда та ін. Київ: НУОУ ім. Івана Черняховського, 2020. 328 с.

3. Концепція зовнішньої політики України. Експертні рекомендації / Під загальною ред. Є. Габер, С. Корсунського, Г. Шелест. Вид-во Фонду ім. Фрідріха Еберта. 2020. 108 с.

4. Кутідзе Л. С. Проблеми побудови механізмів диверсифікації експортного потенціалу регіону. *Technology audit and production reserves*. 2017. № 1(7). С. 32–36.

5. Петько С. М. Глобалізація як основа світових інтеграційних процесів. *Экономика. Финансы. Право:* інформаційно-аналітичний журнал ; засн. Аудиторська фірма «Аналітик», Академія муніципального управління ; гол.ред. В.К. Присяжнюк. Київ, 2013. № 11/1. С. 22–24.

URI: https://ir.kneu.edu.ua:443/handle/2010/39390

6. Петько С. М. Сутність та значення економічної інтеграції в глобальній економіці. *Буковинський університет: зб. наукових праць. Економічні науки*. Вип. 10. Чернівці : Книги-ХХІ, 2014. С. 188–194.

URI: https://ir.kneu.edu.ua:443/handle/2010/39454

7. Петько С. М. Технології індустрії 4:0 у цифровій парадигмі розвитку глобальної економіки. *Економічний вісник НТУУ «КПІ».* 2022. № 24. DOI: https://doi.org/10.37734/2409-6873-2022-2-9

Секція 2
ІНФОРМАЦІЙ І ТЕХНОЛОГІЇ

УДК 004.896=111

ARTIFICIAL INTELLIGENCE AND ITS USE IN MODERN 3D MODELING

Dukov V.O.
Dmytro Motornyi Tavria State Agrotechnological University, Zaporizhzhia

Анотація. Статтю присвячено аналізу інтеграції штучного інтелекту та його імплементації у технічне та інженерне 3D моделювання. Наведено переваги та недоліки використанні штучного інтелекту у 3D моделюванні.

Ключові слова: штучний інтелект, інструменти генеративного проектування на основі ШІ.

Summary. The article is devoted to the analysis of the integration of artificial intelligence and its implementation in technical and engineering 3D modeling. The advantages and disadvantages of using artificial intelligence in 3D modeling are given.

Key words: artificial intelligence, AI-driven generative design tools.

Artificial Intelligence (AI) is being increasingly integrated into modern 3D modeling processes, revolutionizing the way 3D content is created and manipulated. AI's role in 3D modeling encompasses various aspects, from accelerating the design process to enhancing realism and interactivity. There are several ways to use artificial intelligence in the field of both technical and engineering 3D modeling, as well as for performing tasks in the design direction. This study is going to focus on some of them.

First of all, there is 3D Object Recognition. AI-powered computer vision models can recognize and classify objects in 3D space. It is used in applications like augmented reality (AR) and virtual reality (VR) for object tracking, interaction, and scene understanding, and also for reverse engineering if it`s necessary to scan some objects or details.

The next very important AI's application is Generative Design: AI-driven generative design tools can automatically generate 3D models based on high-level input parameters and constraints. These models can be used in architecture, product design, and engineering to optimize structures and create innovative designs. This is important because with the help of AI such as Midjourney (Fig. 1). You can get reference images for further design in case of so-called creative crises of designers; also, ChatGPT (Fig. 2), it can be useful for engineers and mechanics because it can replace a lot of reference books and literature. It has a clear structure and contains a lot of information. Combined with an arbitrary, simple format for information retrieval (simple or complex direct questions directly to the AI) this model is a new breakthrough that can be compared to the advent of the Internet almost 40 years ago.

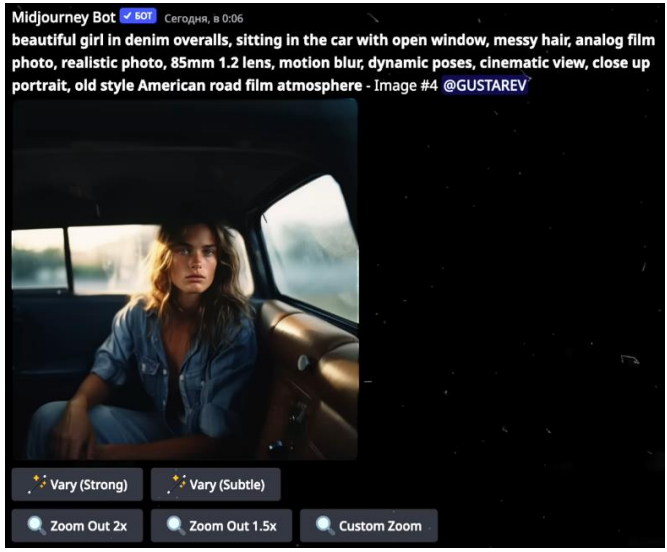


Figure 1. The generation of a non-existent woman with an entourage

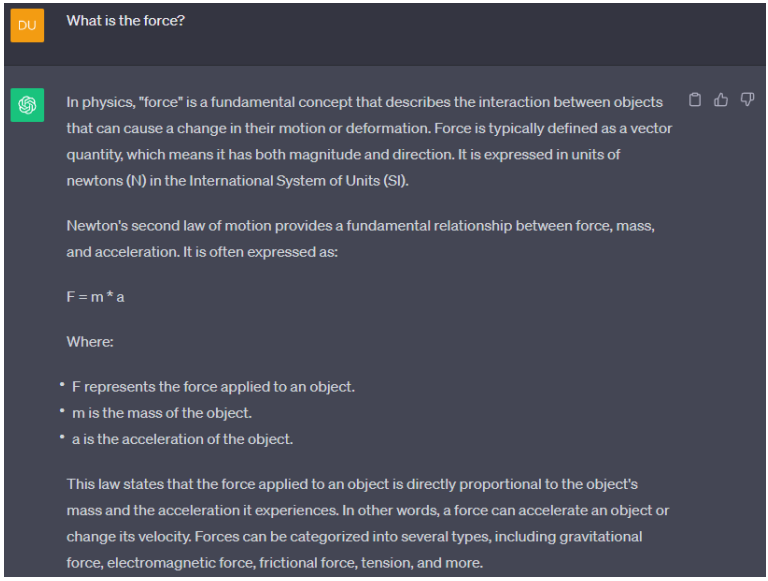


Figure 2 – A question to ChatGPT

The next paramount aspect is texture synthesis and mapping: AI can automate the process of generating and mapping textures onto 3D models, improving the realism and visual quality of 3D scenes and characters.

Similar AI mechanisms have been incorporated into such technologies as:

1. Nvidia RTX (Ray Tracing Texel eXtreme) which includes the creation of rays and reflections in real time using algorithms of video chips and not their direct computing power, in order to reproduce them directly in games and improve the overall performance of systems as well as visual qualities using additional resources.
2. DLSS which uses similar algorithms to generate intermediate frames and dynamic changes in real time for games, videos, and other graphic content.
3. RDNA – an analogue of Nvidia RTX for systems with AMD Radeon which also has its own advantages in terms of image scaling and the use of tensor kernels for ray tracing and real-time systems.

It is reasonable to highlight the main conclusions regarding the modern use of AI in modeling. The negative points are:

- lack of clear control of the reliability of information due to the existing model of the existence of AI;
- the possibility of causing harm on the part of the user by entering inaccurate information into the specific AI databases which leads to total failures as well as the use of incorrect information by people with the corresponding consequences;
- misuse of information by students and teachers of educational institutions.

The positive points are:

- mobility of AI systems (most of them are online services operated by servers);
- flexibility of creation and usually open source for other developers;
- centralization of all data into one network and a complete system, which is a good optimization for work in modern times;
- the ability to solve both non-trivial problems and trivial ones on which a person would spend an inordinate amount of time.

Література

1. Max Tegmark «Life 3.0: Being Human in the Age of Artificial Intelligence» 2017, 384 p.
2. MidJourney review v5.2: website. URL: https://www.youtube.com/watch?v=MVqC1S0QrHE&ab_channel=MaximGustarev (Last accessed 03.11.2023)
3. Official AI RTX Technologies: website. URL: https://www.nvidia.com/en-us/design-visualization/technologies/rtx/ (Last accessed 03.11.2023)

УДК 004.896=111

ARTIFICIAL INTELLIGENCE IN ENGINEERING

Valieva K.M.
Dmytro Motornyi Tavria State Agrotechnological University, Zaporizhzhia

Анотація. Статтю присвячено аналізу сучасного стану розвитку штучного інтелекту та його імплементації у такі галузі як промислове виробництво, аерокосмічний сектор, туризм, транспортна система.

Ключові слова: штучний інтелект, алгоритми машинного навчання, скорочення примусового простою.

Summary. The article deals with the analysis of the current state of artificial intelligence development and its implementation in such areas as industrial production, the aerospace sector, tourism, and the transport system.

Key words: artificial intelligence, machine learning algorithms, reducing downtime.

Artificial intelligence (AI) is rapidly becoming an important tool for engineers to solve complex problems and automate processes. One of the most important applications of AI in technology is in the manufacturing business. Engineers are using machine learning algorithms to improve manufacturing operations, minimise downtime, and increase efficiency. For example, AI-driven applications can evaluate data from production lines in real time to predict and prevent equipment failures and increase productivity. Another area where AI is having a major impact is transport. Engineers are using deep learning algorithms to improve the performance and safety of self-driving cars. Artificial intelligence is truly shaping the future of the autonomous vehicle industry. Cars are equipped with sensors that constantly monitor everything that happens around the car and make the right adjustments using artificial intelligence. These sensors capture thousands of data points every millisecond (e.g. car speed, road conditions, pedestrian locations, other traffic, etc.) and use artificial intelligence to help interpret the data and act accordingly - all instantly. These algorithms can make accurate predictions and improve the performance of autonomous vehicles. Artificial intelligence is becoming a trend in tourism, which is directly related to the transport sector. Artificial intelligence makes travelling easier, from organising trips to suggesting the most efficient route home after work. Advanced industries such as AI are driving the growth of the global travel technology market, which is expected to reach $12.5 billion by 2026 [1]. In fact, AI is seen as a tool that can give travel companies a competitive edge, so customers can expect to interact with AI more frequently during future travels. Artificial intelligence is also used in the aerospace sector to improve aircraft design and performance. Engineers use machine learning algorithms to evaluate

wind tunnel and flight test data to improve aircraft designs. This improves performance and reduces fuel consumption and emissions. Engineers in the energy sector use artificial intelligence to optimise the production and delivery of electricity. For example, engineers are using neural networks to detect and avoid power failures, reduce downtime, and improve grid reliability. One of the most promising applications of artificial intelligence in technology is materials science. Engineers use machine learning algorithms to validate test and simulation data to identify new materials and improve the quality of existing ones. This can contribute to the development of new products and services, such as creating stronger, lighter, and more durable materials.

In summary, the use of artificial intelligence has made engineering more automated, covering industries such as transport, energy, aerospace and manufacturing. The use of artificial intelligence will only continue to grow as engineers continue to discover new ways to apply AI to solve complex problems. In particular, AI can create new opportunities for economic growth and job creation.

Література

1. Global Travel Technologies Market to Reach $12.5 Billion by 2026: website. URL: https://www.prnewswire.com/news-releases/global-travel-technologies-market-to-reach-12-5-billion-by-2026--301508644.html (Last accessed: 13.10.2023)

УДК : 004.9

WEB SCRAPING AS A MODERN METHOD OF AUTOMATIC INFORMATION COLLECTION

Vaskovskyi Artem, Symonenko Svitlana
Dmytro Motornyi Tavria State Agrotechnological University, Zaporizhzhia

Анотація. У статті розглядаються основні методи автоматичного збору інформації з веб-сторінок з використанням мови програмування Python, описано їх недоліки і переваги. Розглянуто бібліотеки, що дозволяють здійснювати ефективний збір інформації.

Ключові слова: збір інформації, мова програмування Python, веб-сторінки.

Summary. The article discusses the main methods of automatic information collection from web pages using the Python programming language, describes their disadvantages and advantages. Libraries that allow for effective information collection are considered.

Keywords: information collection, Python programming language, web pages.

There are numerous methods and techniques for information collection. The purpose of this article is to review the main methods of automatic information collection from web pages using the Python programming language with the focus on their advantages and disadvantages and review of libraries that allow users to collect information efficiently.

In today's data-driven world, the ability to gather information from the web quickly and efficiently has become a key skill. Python, with its versatile libraries like Requests and BeautifulSoup, has taken the lead in automating this process with web scraping. In this article, we want to delve into the intricacies of modern web scraping methodologies using the Python programming language and emphasize the potential of asynchronous parsers that greatly speed up this process.

The simplicity of the Python language and its extensive selection of libraries allow developers and data enthusiasts to effortlessly extract valuable information from websites. The Requests library is a powerful tool that makes it easy to extract HTML content from URLs (the HTML file is where all the content of a web page is stored). Its user-friendly interface simplifies the extraction process by making it easy to make HTTP requests and process the responses.

But data can be obtained not only from HTML content, but also through API (Application Programming Interface). Basically API is a set of rules and protocols for building and interacting with software applications. It is like a menu in a restaurant. The menu provides a list of dishes a customer can order, along with a description of each dish. When customer specify what menu items they want, the restaurant kitchen does the work and provides customers with some finished dishes. Customers do not know exactly how the restaurant prepares that food, and they do not really need to.

Similarly, an API lists a bunch of operations that a programmer can use, along with a description of what they do. The programmer does not necessarily need to know how, for example, Telegram messenger sends messages from one person to another, they just need to know that it is possible to do so using the API.

Usually API returns conveniently collected data in the JSON format. But not all websites have their own API, so in cases where they do not, users have to get the information from the HTML document only.

Once the original HTML content is retrieved, the BeautifulSoup library comes in and performs powerful syntax analysis. Its intuitive syntax and functions such as find() and find_all(), as well as its extensive features, allow users to extract specific data elements from the HTML structure. Using a variety of methods and selectors, BeautifulSoup simplifies the extraction process by allowing users to efficiently navigate throughout the HTML document and collect data.

While Requests and BeautifulSoup are quite powerful ways to gather information, the need for speed and efficiency led to the advent of asynchronous parsing. Asynchronous programming in Python using libraries such as Aiohttp and Asyncio is revolutionizing web scraping by allowing tens and hundreds of requests to be executed simultaneously, respectively parsing tens and hundreds of web pages at a time, greatly increasing efficiency.

Aiohttp and Asyncio paired together can achieve very impressive results in collecting huge amounts of information in a matter of seconds.

Aiohttp, a well-known asynchronous HTTP client-server framework, optimizes the web scraping process by enabling simultaneous execution of HTTP requests. Asynchrony provides non-blocking operations, which means that as soon as a request has been sent to a website, the program will not stop and wait for a response from the website, it will continue its execution and send new requests. This significantly reduces the waiting time and increases the speed of operation, which makes it indispensable for large-scale data extraction projects.

The Asyncio library itself in its turn serves as a foundation for implementing asynchronous tasks on it. It provides a basis for writing parallel code using async/await syntax. When combined with Aiohttp Asyncio provides seamless coordination of concurrent execution of multiple web scraping tasks, taking advantage of the asynchronous programming paradigm.

Using asynchronous parsing in web scraping offers a lot of benefits:

- Increased speed: simultaneous execution of HTTP requests significantly reduces latency, resulting in faster data retrieval.
- Scalability: asynchronous parsing allows more requests to be processed simultaneously, making it possible to search huge amounts of data.
- Resource efficiency: optimal resource utilization through non-blocking operations minimizes resource wastage and increases efficiency.

– Improved performance: asynchronous parsing provides a smoother and more responsive scraping process, especially when dealing with a large number of sites or high data load.

While it may seem that asynchronous parsing has many advantages, it also has disadvantages:

– A very heavy load on the site from which the information is collected. This can slow down the site for other users and even lead to the blocking of your IP address by site administrators.
– Complexity: asynchronous programming is usually more complex than synchronous programming. Tasks such as error handling, task synchronization, and data sharing may be more complex in an asynchronous context.
– Debugging complexity: debugging asynchronous code can be difficult. Traditional debugging tools may not handle asynchronous code as expected, and errors may be more difficult to reproduce and correct.
– Unpredictable execution order: In asynchronous programming, tasks are executed in parallel rather than sequentially. This means that the order of execution of tasks can be unpredictable, which can lead to problems if the tasks depend on each other.

Taking all of the above into account, we can conclude that Python, combined with libraries such as Requests, BeautifulSoup, Aiohttp, and Asyncio, is a powerful toolkit for modern web scraping. By integrating asynchronous parsing techniques, the efficiency and speed of retrieving information from the web can be improved.

References

1. How to Scrape Websites Without Getting Blocked. URL: https://www.scrapehero.com/how-to-prevent-getting-blacklisted-while-scraping/.

2. Async IO in Python: A Complete Walkthrough. URL: https://realpython.com/async-io-python/.

3. How To Work with Web Data Using Requests and Beautiful Soup with Python 3. URL: https://www.digitalocean.com/community/tutorials/how-to-work-with-web-data-using-requests-and-beautiful-soup-with-python-3.

4. Ultimate Guide to Web Scraping with Python Part 1: Requests and BeautifulSoup. URL: https://www.learndatasci.com/tutorials/ultimate-guide-web-scraping-w-python-requests-and-beautifulsoup/.

5. Requests: HTTP for Humans™. URL: https://requests.readthedocs.io/en/latest/.

6. Beautiful Soup Documentation. URL: https://www.crummy.com/software/BeautifulSoup/bs4/doc/.

УДК 004.93:351.862

ЗАСТОСУВАННЯ АЛГОРИТМУ YOLO ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ ОБ'ЄКТАМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У РЕЖИМІ РЕАЛЬНОГО ЧАСУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Азаров Іван, Гнатюк Сергій, Сидоренко Володимир, Азаров Ілля
Національний авіаційний університет,
Інститут державного управління та наукових досліджень з цивільного захисту

Проаналізовано існуючі алгоритми машинного навчання. Зазначається, що для захисту об'єктів критичної інфраструктури алгоритм YOLO може бути більш придатними для виявлення об'єктів в умовах реального часу. Наведено приклад виявлення вогню та диму алгоритмом YOLO. Розроблена матриця плутанини показує, що при збільшенні кількості тренувань збільшується якість та зменшується кількість помилок у впізнанні вогню та диму.

Ключові слова: алгоритми машинного навчання, гібридна війна, небезпека, загрози, об'єкти критичної інфраструктури.

Existing machine learning algorithms are analyzed. It is noted that for the protection of critical infrastructure objects, the YOLO algorithm may be more suitable for detecting objects in real-time conditions. An example of fire and smoke detection by the YOLO algorithm is given. The developed confusion matrix shows that with an increase in the number of trainings, the quality increases and the number of errors in fire and smoke recognition decreases.

Keywords: machine learning algorithms, hybrid warfare, danger, threats, critical infrastructure objects.

В умовах масштабної гібридної війни в Україні зростає кількість кіберзагроз, під загрозою опиняються життя і здоров'я громадян та цілісність критично важливих об'єктів (КВО), тому вчорашні надійні технології потребують швидкого вдосконалення, модернізації та якісного тестування. Для уникнення людських помилок з'являються та розвиваються технології машинного навчання (МН). Алгоритми МН стають все більш популярними для виявлення у режимі реального часу небезпек і загроз, такі як вогонь, дим, авіаційна та ракетна загроза КВО цивільної та військової інфраструктури.

В умовах війни традиційні методи виявлення пожежі, такі як детектори диму та теплові камери можуть займати відносно багато часу та бути не завжди точними. Алгоритми МН у режимі реального часу можуть швидко і точно виявляти пожежі, аналізуючи зображення з камер. Це дозволяє швидше реагувати та запобігати пошкодженню та ураженню КВО та травмуванню персоналу. Також алгоритми МН можуть швидко й точного виявити та відстежити літаки і БПЛА у режимі реального часу за допомогою відеокамер, які потенційно можуть використовуватися для зловмисних цілей, таких як шпигунство або терористичні атаки. Це може допомогти в управлінні повітряним рухом і підвищити безпеку КВО.

Алгоритми МН довели свою високу ефективність у виявленні потенційних загроз і забезпеченні раннього попередження і нейтралізації для запобігання потенційним лихам в умовах масштабної війни в Україні.

Слід зазначити, що найкращий алгоритм для певної програми залежить від конкретних вимог завдання та наявного апаратного забезпечення. Загалом, під час вибору алгоритму виявлення об’єктів у реальному часі необхідно знайти компроміс між швидкістю, точністю та обчислювальними ресурсами. Під час вибору алгоритму виявлення об’єктів у режимі реального часу важливо враховувати специфічні вимоги програми, такі як тип об’єктів, що підлягають виявленню, розмір об’єктів, складність сцен та необхідна швидкість обробки. Крім того, також важливо враховувати доступні обчислювальні ресурси та доступність даних.

Наприклад, якщо потрібно виявити невеликі об’єкти або детальні класи у програмі реального часу, такі алгоритми як RetinaNet, Faster R-CNN, R-FCN, Mask R-CNN, EfficientDet можуть бути більш придатними, оскільки вони мають вищу точність для цих типів об'єктів, але можуть вимагати більше обчислювальних ресурсів і не такі швидкі як інші аналоги. Такі алгоритми як YOLACT, CornerNet, CenterNet можуть обробляти інформацію швидше, вимагають менших затрат обчислювальних ресурсів, але мають найнижчу точність детекції невеликих об’єктів. А такі алгоритми, як YOLO та SSD, можуть бути більш прийнятними і придатними для виявлення об'єктів за зображеннями, а також відео в умовах реального часу і веб-камерами на малопотужних пристроях і з обмеженими обчислювальними ресурсами. Приклади виявлення об'єктів показані на рисунках 1 і 2.

Рисунок 1 – Приклад виявлення вогню алгоритмом YOLO

Рисунок 2– Приклад виявлення диму алгоритмом YOLO

Для захисту КВО оптимальним рішенням буде використання алгоритму YOLO [1]. Швидкість навчання цієї нейронної мережі висока, вона не потребує великої кількості обчислювальних ресурсів і має достатньо гарну точність. Ознайомитися з матрицею плутанини, яка показує, що при збільшенні кількості тренувань збільшується якість та зменшується кількість помилок у впізнанні вогню та диму, можна на рис. 3.

Швидкість, точність і ціна на обчислювальне обладнання визначають оптимальність використання, тому що ці критерії обумовлюють швидкість прийняття рішення ситуаційним центром для знешкодження потенційних загроз та збереження життя і здоров’я людей.

Алгоритм YOLO можна швидко навчити виявляти потрібні об’єкти за обмежений час. Він має гарну точність знаходження небезпечних об’єктів, яка залежить від якості і кількості етапів навчання, та не потребує великих серверних потужностей (також можна використовувати і хмарні серверні обчислення).

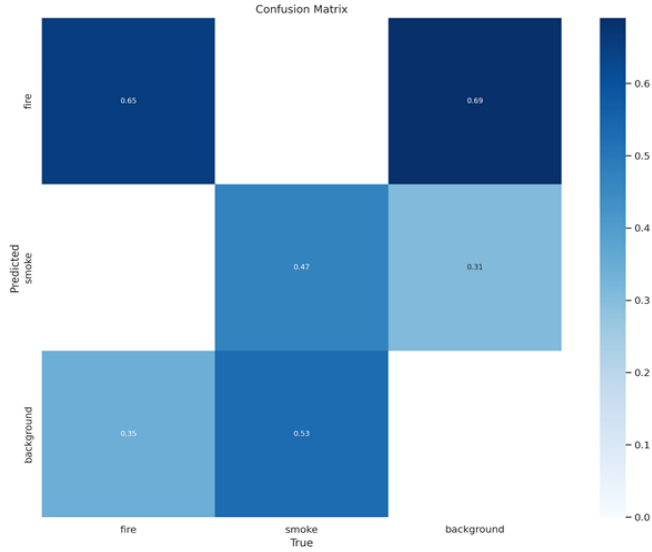


Рисунок 3 – Матриця плутанини

Слід зазначити, що алгоритми МН не є досконалими, і результати повинні перевірятися фахівцями ситуаційного центру і обробки інформації, які зможуть оцінити якість навченої моделі на знаходження об’єктів та покращити якість алгоритмічної моделі збільшивши кількість етапів навчання.

Алгоритми МН можна використовувати разом або комбінувати їх і поєднувати за допомогою ансамблевих методів (наприклад, використовувати кілька алгоритмів для швидшого і точнішого навчання загальної моделі), що може підвищити загальну продуктивність системи. Це особливо важливо під час захисту КВО, де невеликі помилки можуть призвести до великих катастроф.

Література

1. I. Azarov, S. Gnatyuk, M. Aleksander, I. Azarov and A. Mukasheva. Real-time ML Algorithms for The Detection of Dangerous Objects in Critical Infrastructures. IntelITSIS’2023: 4th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 22–24, 2023, Khmelnytskyi, Ukraine.

УДК 377.004.8

ІНТЕГРАЦІЯ ТРИВИМІРНОГО КЛАСУ В НАВЧАЛЬНИЙ ТЕЛЕГРАМ БОТ ЯК ІНСТРУМЕНТ ДЛЯ ПРОВЕДЕННЯ ПРАКТИЧНИХ ЗАНЯТЬ В УМОВАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Андрощук Олександр, Гуменюк Микола
Вище професійне училище Львівського державного університету безпеки життєдіяльності (м. Вінниця)

Анотація. У тезах висвітлено можливості використання інтерактивних симуляцій та інших мультимедійних засобів для поліпшення навчання, а також використання віртуальної реальності та розширеної реальності в освітніх цілях. Основний акцент матеріалу зроблено на інтеграції тривимірного класу в навчальний телеграм-бот. Пояснюється, як така інтеграція може поліпшити освітній процес. Надано послідовний план створення чат-бота в Telegram для інтерактивної взаємодії з сферичними панорамними фотографіями, від створення бота і завантаження фотографій до інтеграції інтерфейсу програмування додатків та створення команд для користувачів.

Ключові слова: електронні платформи; дистанційне навчання; тривимірний клас; телеграм-бот; сферична панорама; інтерфейс програмування додатків; інтерактивні можливості.

Keywords: electronic platforms; distance learning; three-dimensional class; telegram bot; spherical panorama; application programming interface; interactive capabilities.

Розвиток електронних платформ для навчання - це сегмент освіти, який відображає сучасні тенденції та вимоги до навчальних систем. Особливо під час глобальних криз, таких як пандемія COVID-19, дистанційне навчання стало популярним і ефективним засобом навчання. Електронні платформи для навчання надають можливість здобувачам освіти навчатися з будь-якого місця та в будь-який час.

Штучний інтелект використовується для аналізу навчальних даних, автоматичної оцінки студентів, рекомендацій і взаємодії з користувачами для покращення навчання.

Платформи надають багато можливостей для використання відео, аудіо, інтерактивних симуляцій та інших мультимедійних засобів для поліпшення навчання та зрозуміння матеріалу. Віртуальна реальність та розширена реальність дозволяють створювати інтерактивні навчальні дослідження, симуляції та віртуальні тури. Сучасні платформи навчання повинні бути доступними на мобільних пристроях, оскільки багато студентів навчаються на смартфонах та планшетах.

Ці тенденції відображають зростання інтересу до електронних платформ для навчання та їхню ефективність у сучасному освітньому середовищі.

Інтеграція тривимірного класу в навчальний телеграм бот може бути корисним інструментом для покращення освітнього процесу. Для цього можна використовувати спеціалізовані бібліотеки та інструменти для віртуальної реальності або тривимірного моделювання.

За допомогою цієї інтеграції здобувачі освіти можуть:

1. Досліджувати тривимірні об'єкти та середовища в режимі реального часу.
2. Вивчати складні концепції, в інтерактивному форматі.
3. Проводити віртуальні екскурсії або лабораторні роботи в тривимірному просторі.
4. Виконувати завдання та тести, пов'язані з тривимірними об'єктами.

Для реалізації цього, необхідно розробити спеціального бота та інтегрувати зі спеціалізованими інтерфейсами програмування додатків (API) для тривимірного моделювання.

Створення чат-бота в Telegram, який інтегрується з сферичною панорамою, може дати користувачам можливість взаємодіяти зі сферичними фотографіями та отримувати інформацію про них через чат.

Ось, як це може працювати:

1. Створення бота в Telegram. Спочатку створюється Telegram-бот. Це можна зробити через @BotFather в Telegram.
2. Завантаження сферичних фотографій. Завантажуються сферичні панорамні фотографії на платформу чи сервер, який підтримує відправку зображень через API.
3. Інтеграція API для сферичних фотографій. Створення API, який дасть можливість чат-боту отримувати та відображати сферичні фотографії в Telegram.
4. Створення команд для бота. Додавання команд до бота, які дозволять користувачам запитувати конкретні сферичні фотографії або інформацію про них.
5. Відповідь на запити користувачів. Коли користувачі відправляють команди або запити, бот може відправляти відповіді, які містять сферичні фотографії або пояснення про них.
6. Інтерактивні можливості. Взаємодія з фотографіями, наприклад, розширення або відображення додаткової інформації при кліку на певну область фотографії.
7. Збереження прогресу та інші функції. Залежно від застосування, можливо також зберігати прогрес користувачів, надавати можливість взаємодіяти з іншими користувачами і так далі.

Описана інтеграція забезпечить користувачів можливістю досліджувати та взаємодіяти з сферичними панорамами через Telegram-чат.

Висновок. Як підсумок, варто відмітити, що синтез телеграм-бота та тривимірного зображення відкриває широкі можливості для освіти та інтерактивного навчання. Це дозволяє здобувачам освіти взаємодіяти з

навчальним матеріалом, натискаючи на кнопки та виконуючи дії в тривимірному середовищі. Тривимірні зображення можуть візуалізувати складні концепції та об'єкти, що полегшує їх розуміння і запам'ятовування. Telegram забезпечує доступ до тривимірних зображень та навчального матеріалу в будь-який час та з будь-якого місця. Ця інтеграція може використовуватися для проведення практичних занять, на кшталт перевірки протипожежного стану об'єкта, що дозволяє здобувачам освіти набути практичних навичок у безпечному віртуальному середовищі. Тому ця інтеграція робить навчання більш інтерактивним, доступним і ефективним, дозволяючи здобувачам освіти краще розуміти та набувати навички.

Література

1. Системи обробки інформації. [Електронний ресурс] // hups.mil.gov.ua – 2019. – Режим доступу: http://www.hups.mil.gov.ua/periodic-app/article/19319 2.

2. Types of Chatbots. Rule-Based Chatbots vs AI Chatbots. [Електронний ресурс] // mindtitan.com – 2020. – Режим доступу: https://mindtitan.com/resources/ guides/chatbot/types-of-chatbots/.

3. Як створювати й публікувати кругові панорами на Картах Google. [Електронний ресурс] // https://support.google.com/. – Режим доступу: https://support.google.com/maps/answer/7012050?hl=uk.

4. Інтеграція за допомогою API: що це таке, її функції та можливості у продуктах InBase. [Електронний ресурс] // https://www.inbase.com.ua/. – Режим доступу: https://www.inbase.com.ua/ua/blog/intehratsiia-za-dopomohoiu-api-shcho-tse-take-ii-funktsii-ta-mozhlyvosti-u-produktakh-inbase.html.

5. Five Different Types of Chatbot. [Електронний ресурс] // medium.com – 2019. – Режим доступу: https://medium.com/voiceui/five-different-types-ofchatbot17bb255b23b4.

6. ТОП 10 Найбільш популярних месенджерів України та світу. [Електронний ресурс] // eo-marketing.com.ua – 2020. – Режим доступу: https://seomarketing.com.ua/ top-10-naibilsh-populiarnykh-mesendzheriv-ukrainy-ta-svitu/.

УДК 004.738.5

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ДЛЯ ЦИРКУЛЯЦІЙНО-ЦІННІСНОГО УПРАВЛІННЯ ПРОЕКТАМИ ЕНЕРГОЗАБЕЗПЕЧЕННЯ ЖИТЛОВИХ МАСИВІВ

Андрушків Олег
Львівський державний університет безпеки життєдіяльності

Проаналізовано сучасний стан житлових масивів, які є складними інфраструктурними системами, та визначено доцільність ефективного управління проектами їх енергозабезпечення. Подано задачі, які вирішуються під час управління енергопостачанням житлових масивів на підставі сучасних інформаційних технологій. Означено доцільність використання сучасних інформаційних технологій для циркуляційно-ціннісного управління проектами енергозабезпечення житлових масивів, їх приклади та переваги.

Ключові слова: інформаційні технології, управління, проекти, енергозабезпечення, житлові масиви

The current state of residential areas, which are complex infrastructural systems, was analyzed, and the expediency of effective management of their energy supply projects was determined. The tasks that are solved during the management of the energy supply of residential areas on the basis of modern information technologies are presented. The expediency of using modern information technologies for circulation and value management of energy supply projects of residential areas, their examples, and advantages are determined.

Keywords: information technologies, management, projects, energy supply, residential areas

Сучасні житлові масиви є складними інфраструктурними системами, які потребують ефективного управління енергопостачанням. Це пов'язано з такими факторами, як зростання енергоспоживання, необхідність впровадження енергозберігаючих технологій, а також підвищення вимог до якості та надійності енергопостачання. При цьому інформаційні технології відіграють важливу роль в управлінні енергопостачанням житлових масивів. Вони можуть використовуватися для вирішення низки завдань, які представлено на рисунку 1.

Збір та аналіз даних про енергоспоживання здійснюється із використанням сучасних інформаційних технологій, які можуть збирати дані про споживання енергії з різних джерел, таких як датчики, лічильники, а також системи автоматизації. Це дозволяє отримувати точну та актуальну інформацію про енергоспоживання, яка може використовуватися для прийняття рішень щодо підвищення ефективності енергопостачання.

Інформаційні технології використовують для моніторингу та контролю за роботою енергосистем. Це дозволяє виявляти проблеми та збої в роботі системи на ранніх стадіях, що забезпечує уникнення аварій та зменшення ризиків для населення.

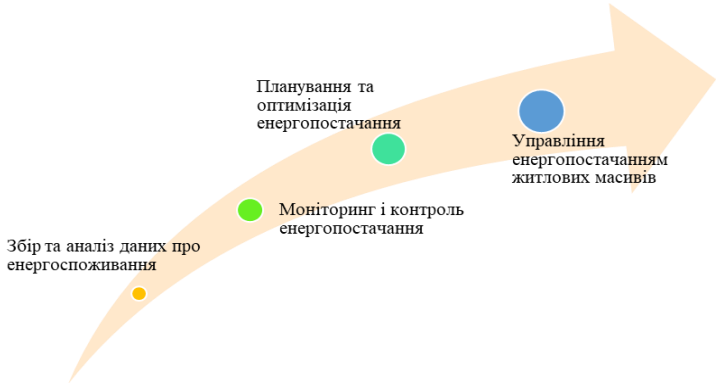


Рисунок 1 – Задачі, які вирішуються під час управління енергопостачанням житлових масивів на підставі сучасних інформаційних технологій

Управління енергопостачанням житлових масивів за використання циркуляційно-ціннісного підходу має на меті не лише забезпечення ефективного і надійного енергопостачання, але й мінімізацію негативного впливу на навколишнє середовище та підвищення якості життя населення завдяки використання відходів, що ними продукуються.

Сучасні інформаційні технології є невід'ємною складовою ефективного планування та оптимізації процесів енергопостачання (табл. 1). Вони дозволяють забезпечити оптимальне використання енергоресурсів та мінімізувати витрати на енергопостачання.

Таблиця 1 – Сучасні інформаційні технології для циркуляційно-ціннісного управління проектами енергозабезпечення житлових масивів

Сучасні ІТ-технології	Приклад застосування ІТ-технології	Переваги
Інтернет речей (IoT)	Використання датчиків та інших пристроїв IoT для збору даних про проектне середовище.	Дозволяє отримувати точні та актуальні дані про енергоспоживання, які можуть використовуватися для проектних менеджерів.
Машинне навчання та штучний інтелект	Використання машинного навчання та штучного інтелекту для аналізу даних про енергоспоживання, виявлення тенденцій та прогнозування майбутнього споживання енергії.	Дозволяє підвищити точність прогнозування енергоспоживання, що може допомогти в плануванні та оптимізації енергопостачання.
Розробка та впровадження нових енергоефективних рішень	Використання ІТ-технологій для моделювання та симуляції різних сценарії проектів, що дозволяє оцінити їх ефективність та економічну доцільність.	Дозволяє розробляти та впроваджувати найбільш ефективні та економічно доцільні сценарії реалізації проектів.
Розумні мережі	Використання розумних мереж для автоматизації управління проектами	Дозволяє підвищити ефективність та точність управління проектами, а також зменшити їх ризики.

З таблиці 1 можна зазначити, що сучасні інформаційні технології мають значний вплив на підвищення ефективності проектів та їх продуктів. Вони можуть використовуватися для вирішення широкого спектру управлінських завдань, таких як збір і аналіз даних, моніторинг і контроль, планування та оптимізація, а також забезпечення якісних продуктів проектів – енергоефективності житлових масивів із використанням відходів, що продукує їх населення.

Подальші дослідження слід проводити із розробки методів та моделей, які лежатимуть в основі розробки інформаційних технологій для циркуляційно-ціннісного управління проектами енергозабезпечення житлових масивів. Саме вони забезпечать отримання ефективних та точних управлінських рішень. Застосування інформаційних технологій для циркуляційно-ціннісного управління проектами енергопостачання житлових масивів є перспективним напрямком, що забезпечить підвищення ефективності та надійності енергопостачання, зменшення негативного впливу на навколишнє середовище та підвищення якості життя населення.

Література

1. Eurostat. Waste Statistics – Database. European Commission. 2023. Retrieved from https://ec.europa.eu/eurostat/web/waste/data/database

2. Tryhuba, A. et al. Assessment of the Condition of the Project Environment for the Implementation of Technologically Integrated Projects of the “European Green Deal” Using Maize Waste. Energies 2022, 15, 8220.

3. Tryhuba A.; Hutsol T.; Tryhuba I.; Pokotylska N.; Kovalenko N.; Tabor S.; Kwasniewski D. Risk Assessment of Investments in Projects of Production of Raw Materials for Bioethanol. Processes 2021, 9, 12. https://doi.org/10.3390/pr9010012

4. Tryhuba, I., Hutsol, T., Tryhuba, A., Cieszewska, A., Kovalenko, N., Mudryk, K., Glowacki, S., Bry´s, A., Tulej, W., Sojak, M. An Approach to Assessing the State of Organic Waste Generation in Community Households Based on Associative Learning. Sustainability. 2023, 15, 15922.

УДК 614.8

МОДЕЛЮВАННЯ ПРОЦЕДУРИ ФОРМУВАННЯ ШЛЕЙФІВ СИСТЕМ ПОЖЕЖНОЇ СИГНАЛІЗАЦІЇ

Антошкін О.А., Пономарьов К.А.
Національний університет цивільного захисту України, м. Харків

Анотація: В роботі розглядається варіант розв'язання задачі оптимізації складу шлейфів систем пожежної сигналізації як задачі покриття з формуванням з'єднувальної мережі.

Ключові слова: система пожежної сигналізації, задача покриття, розміщення пожежних сповіщувачв, шлейф пожежної сигналізації.

Abstract: The paper considers a variant of solving the problem of optimizing the composition of loops of fire alarm systems as a covering problem with the formation of a connecting network.

Key words: fire alarm system, coverage task, placement of fire detectors, fire alarm loop.

Процес забезпечення життєдіяльності будь-якого об'єкту (будівлі) передбачає, в тому числі, забезпечення пожежної безпеки на ньому. Одним з технічних рішень, яке дозволяє суттєво зменшити час виявлення пожежі, час її вільного розвитку і, як наслідок, збитки від неї, є автоматична система пожежної сигналізації (СПС) [1].

В загальному вигляді задачу проектування СПС можна віднести до класу задач покриття [2] в яких визначену область необхідно повністю покрити визначеними покривними об'єктами з відомими геометричними характеристиками. В якості області покриття Ω представимо приміщення, для якого проектується СПС, а в якості покривних об'єктів – кола T_i, $i = 1, \ldots, n$, зони, що контролюються точковими пожежним сповіщувачами (ПС) [1].

Але слід зазначити, що проектування СПС складається з двох етапів:

- визначення кількості та місць розміщення ПС з урахуванням додаткових обмежень;
- трасування шлейфів пожежної сигналізації.

І якщо розв'язання задачі першого етапу з оптимізацією кількості ПС було розглянуто в ряді робіт, наприклад в [3], то питання формування шлейфів з оптимізацією їх довжини потребує додаткових досліджень.

Обмін інформацією між ПС та приладом приймально-контрольним пожежним (ППКП) в більшості сучасних СПС здійснюється по дротяним лініям зв'язку. Під час трасування дротових з'єднань дуже важливим є врахування технологічних обмежень, тому що використовуються два основних види дротових з'єднань: кільцеве в адресних СПС з більшою кількістю сенсорів і тупикове (радіальне) в безадресних, коли з однієї точки (від ППКП) може виходити кілька шлейфів з обмеженою кількістю ПС в кожному.

Задача по формуванню і оптимізації довжини кільцевого шлейфу може бути сформульована як класична задача комівояжера з відповідними методами для розв'язання.

Задачу побудови тупикових (радіальних) шлейфів можна представити у вигляді варіанта задачі маршрутизації (без обов'язкового повернення до початкової точки), якщо інтерпретувати центри кіл як пункти доставки з потребою в 1 одиницю вантажу й обмежити вантажопідйомність транспорту максимальною кількістю ПС у шлейфі.

Література

1. Дерев'янко О.А., Бондаренко С.М., Христич В.В., Антошкін О.А. Системи пожежної та охоронної сигналізації. Текст лекцій. Харків, 2008. 149 с.

2. Yakovlev S., Kartashov O., Podzeha D. Mathematical Models and Nonlinear Optimization in Continuous Maximum Coverage Location Problem. MDPI Computation. 2022. Vol. 10(7). P. 119–134. URL: https:// https://doi.org/10.3390/computation10070119

3. Антошкин А. А., Комяк В. М., Романова Т. Е. Особенности построения математической модели задачи покрытия в системах автоматической противопожарной защиты // Радиоэлектроника и информатика. Харьков : ХНУРЭ. 2001. № 1. С. 75–78.

УДК: 004.75

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРИКЛАДНОГО ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

Бабич Дмитро, Борзов Юрій
Львівський державний університет безпеки життєдіяльності

Розглянуто роль та застосування прикладного та системного програмування у сучасному інформаційному середовищі. Проведено порівняння та аналіз визначних рис системного та прикладного програмування.

Ключові слова: системне програмування, прикладне програмування, програмне забезпечення.

The role and application of applied and system programming in the modern information environment is considered. A comparison and analysis of the salient features of system and application programming has been carried out.

Keywords: system programming, application programming, software.

Системне програмування (або програмування систем**)** — це вид програмування, який полягає у розробці програм, які взаємодіють з системним програмним забезпеченням (операційною системою), або апаратним забезпеченням комп'ютера.

Системне програмування передбачає проектування та розробку комп'ютерних програм, які дозволяють апаратному забезпеченню комп'ютера взаємодіяти з програмістом і користувачем, що веде до ефективного виконання прикладного програмного забезпечення в комп'ютерній системі. Типові системні програми включають операційну систему та мікропрограмне забезпечення, засоби програмування, такі як компілятори, асемблер, підпрограми вводу/виводу, інтерпретатори, планувальник, завантажувачі та лінкери, а також бібліотеки.

Системне програмування є важливою основою в розробці додатків будь-якого комп’ютера, і постійно розвивається зі змінами в апаратному забезпеченні комп'ютера. Цей вид програмування вимагає певного рівня апаратних знань і залежить від обчислювальної машини. Тому системний програміст повинен знати призначене обладнання, на якому програмне забезпечення повинно працювати.

Системне програмування призводить до розробки програмного забезпечення комп'ютерної системи, яке керує та контролює роботу комп'ютера. Коди низького рівня дуже близькі до апаратного рівня і стосуються

таких речей, як регістри та розподіл пам'яті. Системні програми або системне програмне забезпечення координує передачу даних в різних компонентах і займається складанням, зв'язком, запуском і зупинкою програм, зчитуванням з файлів, а також записом у файли.

Системне програмування розширює функції операційної системи і може містити компоненти, такі як драйвери, утиліти та оновлення. Вони дозволяють ефективно керувати апаратними ресурсами, такими як пам'ять, доступ до файлів, операції вводу / виводу, управління пристроями та управління процесами, такі як адміністрування процесів та багатозадачність. Прикладом може слугувати операційна система, яка зазвичай виступає як інтерфейс між користувачем, прикладним програмним забезпеченням та комп'ютерним обладнанням. ОС забезпечує середовище, яке дозволяє користувачам ефективно виконувати інші програми. Функції операційної системи, що складаються з набору системних програм, включають управління зберіганням, обробку файлів, управління пам'яттю, планування процесора та управління пристроями, обробку помилок, управління процесами та інше.

Прикладами програмного забезпечення, розробленого в результаті системного програмування, є реалізація основних частин операційної системи та програм для мережевої роботи. Наприклад, розробка віртуальної пам'яті або драйверів для операційної системи.

Прикладне програмне забезпечення – це програма або група програм, призначена для кінцевих користувачів. Прикладне програмне забезпечення може бути в комплекті із системним програмним забезпеченням або публікуватися окремо. Прикладне програмне забезпечення може просто називатися додатком.

До різних типів прикладного програмного забезпечення належать:

Набір програм: містить кілька програм разом.

Корпоративне програмне забезпечення: звертається до потреб організації та потоку даних у величезному розподіленому середовищі.

Програмне забезпечення для інфраструктури підприємства: надає можливості, необхідні для підтримки корпоративних програмних систем.

Програмне забезпечення для інформаційного працівника: звертається до індивідуальних потреб, необхідних для управління та створення інформації для окремих проектів у відділах.

Програмне забезпечення доступу до вмісту: використовується для доступу до вмісту і вирішує бажання опублікованого цифрового контенту та розваг

Навчальне програмне забезпечення: надає вміст, призначений для використання у навчанні.

Програмне забезпечення для розробки засобів масової інформації: звертається до індивідуальних потреб генерувати та друкувати електронні носії для використання іншими.

Головною відмінністю системного програмування в порівнянні з прикладним програмуванням є те, що прикладне програмне забезпечення призначене для кінцевих користувачів, тоді як результатом системного програмування є програми, які обслуговують апаратне забезпечення або операційну систему, що обумовлює значну залежність такого типу ПЗ від апаратної частини. Слід зазначити, що звичайні прикладні програми можуть використовувати у своїй роботі фрагменти коду, характерні для системних програм, і навпаки, тому чіткої межі між прикладним та системним програмуванням немає. Оскільки різні операційні системи відрізняються як внутрішньою архітектурою, так і способами взаємодії з апаратним та програмним забезпеченням, то принципи системного програмування для різних ОС є відмінними. Тому розробка прикладних програм, які здійснюватимуть одні і ті ж дії на різних ОС, може суттєво відрізнятися.

Література

1. https://www.wiki.uk-ua.nina.az
2. https://uk.theastrologypage.com/system-programming
3. https://uk.theastrologypage.com/application-software

УДК 378.147.88

ПЛАТФОРМА MOODLE ЯК ПЕРСПЕКТИВНИЙ НАПРЯМОК ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ

Бабійчук Ірина, Романюк Наталія
Інститут державного управління та наукових досліджень з цивільного захисту, м. Київ

Анотація. Збільшення потоків наукової інформації в сучасному світі спонукає до пошуку нових, ефективних способів і засобів навчання, що дозволять надавати здобувачу освіти більше інформації та представляти її в яскравішому і доступнішому для сприйняття форматі. Застосування в освітньому процесі інформаційних технологій — є саме тим фактором, який формує новий підхід до процесу навчання, сприяє підвищенню його інтенсивності та якості.

Ключові слова: інформаційні технології навчання, платформа Moodle.

Abstract. The increase in the flow of scientific information in the modern world prompts the search for new, effective methods and means of learning, which will allow providing the learner with more information and presenting it in a brighter and more accessible format. The use of information technologies in the educational process is precisely the factor that forms a new approach to the learning process, contributes to increasing its intensity and quality.

Key words: educational information technologies, the Moodle platform.

Значна кількість сервісів, які сьогодні можна знайти в мережі Інтернет допомагають під час організації освітнього процесу та використовуються, як доповнення до традиційних форм навчання, збільшуючи спілкування викладача та слухача. Це спонукає педагогічного працівника впроваджувати інновації, використовувати та адаптувати новітні технології в навчальний процес.

Більшість таких сервісів, розвинутий набір інструментів для комп'ютеризованого навчання, в тому числі дистанційного, має в своєму розпорядженні платформа для навчання Moodle. Moodle являє собою безкоштовну, відкриту систему, а тому є привабливою для кожного навчального закладу [1].

Ця система є сучасним, прогресивним середовищем, що знаходиться в постійному розвитку. Середовище Moodle дозволяє навчатися у зручний час, освоювати навчальні дисципліни у зручному ритмі та місці. Окрім цього слухачі мають цілодобовий доступ до навчальних матеріалів, що може включати в себе методичне забезпечення, практичні, тестові завдання, лекційні матеріали, електронну бібліотеку. За допомогою такого віртуального середовища можна управляти навчальним контентом. Велика кількість освітніх елементів і ресурсів мають визначену структуру та доповнюють один одного, маючи при цьому свій окремий вигляд і призначення. А нестандартні елементи навчання роблять освітній процес

різноманітним. Отже, всі зусилля спрямовуються насамперед на організацію взаємодії між педагогічним працівником і здобувачем освіти стосовно організації дистанційного навчання, а також для підтримки навчання офлайн [2].

Таким чином окреслюється перспективність використання в освітньому процесі платформи Moodle як для самостійного опанування дистанційних навчальних курсів. Також на платформу слід звернути увагу під час підготовки практичних занять та планування проведення різного виду контрольних заходів щодо засвоєння навчального матеріалу. У той же час зазначаємо, що розробка навчальних курсів на платформі Moodle потребує подальшого удосконалення.

Література

1. Електронний ресурс: https://moodle.org/mod/page/view.php?id=8174 (дата звернення: 17.10.2023).

2. Жерновнікова Я.В., Пятисоцька С.С. Особливості використання платформи Moodle під час вивчення дисципліни «Інформатика». Науково-методичні основи використання інформаційних технологій в галузі фізичної культури та спорту, 2020, №4. URL: https://journals.uran.ua/itfcs/article/view/212067 (дата звернення: 17.10.2023).

УДК 003.26.09

МЕТОДИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Байрак Олександр, Бурак Назарій
Львівський державний університет безпеки життєдіяльності

Технічний захист інформації є невід'ємною складовою сучасного світу технологій, де безпека даних стає все більш важливою з кожним днем. Проаналізовано ключові аспекти технічного захисту інформації, висвітлено виклики та перспективи подальшого розвитку цієї галузі.

Ключові слова: технічний захист інформації, безпека даних, шифрування, управління доступом, мережевий захист, засоби виявлення вторгнень, вразливості.

Technical information security is an integral component of the modern technological world, where data security becomes increasingly crucial with each passing day. Key aspects of technical information security were analyzed, as well as were highlighted the challenges and prospects of further development of this industry.

Key theses: technical information security, data security, encryption, access management, network security, intrusion detection, vulnerabilities.

У сучасну цифрову епоху важливість кібербезпеки для бізнесу неможливо переоцінити. Зі збільшенням залежності від технологій та Інтернету кіберзагрози стають все більш витонченими та частими, створюючи значний ризик для компаній будь-якого розміру.

Визначимо та проаналізуємо основні поняття технічного захисту інформації, включаючи шифрування, ідентифікацію та аутентифікацію, мережевий захист та засоби виявлення вторгнень. Висвітлимо їх важливість у створенні надійного захисту даних.

Шифрування є ключовим аспектом технічного захисту, оскільки воно дозволяє перетворювати звичайний текст або дані у незрозумілий код, який може бути розкодований тільки за допомогою відповідного ключа. Шифрування використовується для захисту конфіденційної інформації під час передачі по мережі або зберігання на пристроях, забезпечуючи конфіденційність даних.

Ідентифікація визначає, хто ви є, тоді як аутентифікація підтверджує цю ідентичність. Технології, такі як паролі, біометричні дані, двофакторна аутентифікація тощо, використовуються для забезпечення доступу лише авторизованим користувачам та захисту від несанкціонованого доступу.

Захист мережі полягає у використанні різних заходів та технологій для захисту мережевих ресурсів від кібератак та неповноважного доступу. Це передбачає застосування файерволів, віртуальних приватних мереж (virtual private network, VPN), інтрузійних систем виявлення та запобігання, а також сегментацію мережі для зменшення ризику порушень безпеки.

Засоби виявлення вторгнень використовуються для моніторингу мережі та систем на предмет незвичайних або підозрілих активностей, що можуть вказувати на потенційні загрози. Ці засоби включають системи журналювання подій, системи детекції аномалій та аналізу поведінки, допомагаючи вчасно виявляти та реагувати на можливі загрози безпеки.

На сьогоднішній день машинне навчання, штучний інтелект та технології блокчейну активно використовуються для підвищення ефективності технічного захисту і протидії кіберзагрозам. Застосування машинного навчання (machine learning, ML) та штучний інтелект (Artificial intelligence, AI) в автоматизованій аналітиці безпеки дозволяє розвивати системи, які можуть виявляти та реагувати на потенційні кіберзагрози навіть без прямого втручання оператора. Це включає виявлення аномальних патернів у величезних потоках даних, розпізнавання підозрілих активностей та прогнозування майбутніх атак. Важливим фактором є також удосконалення самої систем виявлення загроз шляхом використання ML для навчання таких систем реагувати на нові атаки, навіть на ті, які ще не були відомі, шляхом аналізу зразків зловмисного коду та виявлення аномалій у поведінці системи.

Сьогодні набирає популярності технологія блокчейну, яка може бути використана для створення безпеки в транзакціях та зберіганні інформації. Вона забезпечує можливість безпечного обміну даними між сторонами без проміжних посередників, а також захист від зміни чи втрати даних завдяки властивостям стійкості та фіксованості блокчейну. Зокрема, блокчейн може використовуватися для створення цифрових ідентифікаторів, що дозволяють унікально ідентифікувати користувачів та контролювати їх доступ до конфіденційної інформації.

Використання ML та AI для аналізу великих обсягів даних допомагає вчасно виявляти вразливості та швидко реагувати на потенційні загрози безпеки, забезпечуючи ефективну протидію кіберзагрозам, що має прямий позитивний вплив на підвищення ефективності технічного захисту та протидію кіберзагрозам.

Ці технології дозволяють створювати більш автономні та інтелектуальні системи, які можуть адаптуватися до нових загроз та швидко реагувати на них, забезпечуючи високий рівень безпеки даних та мереж.

Таким чином, проаналізовані технології не лише підвищують рівень технічного захисту, а й відкривають нові можливості для створення більш безпечних інформаційних систем у цифровому світі.

Література

1. Top 7 types of data security technology. [Електронний ресурс]. – Доступний з https://www.techtarget.com/searchsecurity/feature/Top-7-types-of-data-security-technology/

2. Information Security: The Ultimate Guide. [Електронний ресурс]. – Доступний з https://www.imperva.com/learn/data-security/information-security-infosec/

3. Cybersecurity vs. Information Security: Is There A Difference? [Електронний ресурс]. – Доступний з https://www.bitsight.com/blog/cybersecurity-vs-information-security/

4. What is Information Security? Principles, Types [Електронний ресурс]. – Доступний з https://www.knowledgehut.com/blog/security/what-is-information-security#principles-of-information-security

УДК 004.75

ПОТЕНЦІЙНЕ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН В УРЯДІ

Балацька Валерія, Побережник Василь, Опірський Іван
Національний університет "Львівська політехніка"

Анотація. Послуги електронного уряду суттєво еволюціонували, від бюрократичної процедури на паперовій основі до цифрових послуг. Електронно оброблені транзакції потребують обмеженої фізичної взаємодії з державною адміністрацією та забезпечують скорочення часу відповіді, підвищену прозорість, конфіденційність і цілісність. Технологія блокчейн покращує багато з перерахованих вище властивостей, оскільки сприяє незмінності та прозорості зареєстрованих транзакцій і може допомогти встановити довіру між учасниками.

Ключові слова: блокчейн, електронний уряд, захист даних, персональні дані.

Abstract. Descri E-government services have evolved significantly, from paper-based bureaucratic procedures to digital services. Electronically processed transactions require limited physical interaction with government administration and provide reduced response time, increased transparency, confidentiality and integrity. Blockchain technology enhances many of the above properties as it promotes immutability and transparency of recorded transactions and can help establish trust between participants.

Keywords: blockchain, electronic government, data protection, personal data.

Блокчейн – це прозорі, захищені від втручання цифрові книги, реалізовані в розподіленій мережі однорангових вузлів, у яких транзакції здійснюються безпечно й зазвичай без схвалення центрального та довіреного органу [1] . Інформація про кожну транзакцію зберігається хешовано в блоках. Кожен блок також містить хеш попереднього блоку і цей ланцюжок блоків називається книгою. Це дозволяє спільноті користувачів записувати транзакції в загальну книгу, щоб ці транзакції не можна було змінити після додавання в блокчейн. Таким чином, блокчейн дозволяють одноранговим вузлам, які не мають довірчих відносин, обмінюватися даними без третіх сторін або посередників. Ці дані можуть відповідати грошам, контрактам, правам власності на землю, медичним і освітнім записам, сертифікатам, купівлі-продажу товарів/послуг або будь-яким іншим транзакціям чи активам, які можна оцифрувати.

Технологія блокчейн, як і в багатьох інших галузях, варто досліджувати на українському просторі електронним урядуванням для сприяння трансформації державного управління та полегшення надання прозорих і безпечних державних послуг. Основною метою застосування

цього технологічного підходу є уникнення використання центрального органу для транзакцій громадян/бізнесу з державними органами, децентралізація збору, зберігання та обробки даних, а також забезпечення цілісності та незмінності даних.

Однак використання технології блокчейн викликає багато проблем щодо конфіденційності, оскільки багато послуг електронного уряду включають персональні дані, які необхідно належним чином захищати, щоб блокчейн не став об'єктом зловмисників, які отримують несанкціонований доступ до даних громадян. Таким чином, запропоновані рішення повинні враховувати правові обмеження, такі як ті, що накладаються Загальним регламентом захисту даних (GDPR) [2], що в Україні на сьогоднішній день взагалі належно не працює і поважати конфіденційність користувачів під час публікації транзакцій у книзі, забезпечуючи при цьому необхідний авторизований доступ до загальнодоступних адміністративних сторон та інших зацікавлених сторін.

На сьогодні дуже важливо, щоб український Уряд доклав багато зусиль, щоб прийняти та запровадити технологію блокчейн у деяких своїх державних службах [3]. Тут варто виділити вагомі переваги технології блокчейн для застосування у державний реєстрах.

1. Прозорість і довіра. Одним із фундаментальних аспектів технології блокчейн є її прозорість. Усі дані, записані в блокчейн, є незмінними та доступними для авторизованих учасників. Така прозорість вселяє довіру до діяльності уряду, оскільки громадяни можуть перевірити достовірність угод і контрактів.

2. Безпека. Безпека має першочергове значення в електронному урядуванні, де конфіденційні дані обробляються регулярно. Криптографічні функції блокчейн забезпечують захист даних, знижуючи ризик кібератак і витоку даних.

3. Розумні контракти. Розумні контракти, що працюють на основі блокчейн, автоматизують і забезпечують виконання угод без посередників. Це не тільки зменшує бюрократію, але й прискорює процеси, роблячи державні послуги більш ефективними.

4. Цифрова ідентифікація. Блокчейн пропонує надійне рішення для управління цифровою ідентифікацією. Громадяни можуть мати безпечну цифрову ідентифікацію, яку можна перевірити, зменшуючи потребу у фізичній документації під час взаємодії з державними установами.

Однією з основних проблем, з якою стикаються уряди, є забезпечення цілісності даних і записів. У традиційних системах дані можуть бути змінені або підроблені, що призводить до проблем з довірою та підзвітністю. Блокчейн із захищеною від втручання книгою пропонує вирішення цієї проблеми. Дані, записані в блокчейн, не можуть бути змінені без узгодження з мережею, що забезпечує вищий ступінь цілісності даних. Це особливо важливо в таких сферах, як медичні записи, юридична документація та земельні реєстри.

Уряди в усьому світі зміщують свою увагу на надання послуг, які більше орієнтовані на громадян. Блокчейн може надати громадянам більший контроль над своїми даними та взаємодією з державними установами. Наприклад, громадяни можуть мати доступ до своїх особистих даних у блокчейн, дозволяючи їм надавати або скасовувати доступ державним установам або третім особам, залежно від їхніх потреб і уподобань. Це не тільки покращує конфіденційність даних, але й сприяє розвитку почуття власності та розширення можливостей серед громадян.

Блокчейн не обмежується внутрішнім управлінням, він має потенціал революціонізувати міжнародну торгівлю та управління ланцюгом поставок. Розумні контракти дозволяють автоматизувати весь процес торгівлі, від виставлення рахунків до митного оформлення. Це не тільки зменшує паперову роботу та бюрократію, але й підвищує безпеку та прозорість транскордонних операцій.

Уряди, які використовують блокчейн, часто вважаються лідерами інновацій. Це приваблює підприємства та стартапи до регіону, сприяючи процвітаючій екосистемі технологій та підприємництва. Наприклад, блокчейн-стратегія Дубай спрямована не лише на трансформацію державних послуг, але й на позиціонування міста як глобального центру блокчейн-інновацій. Така ініціатива може стати магнітом для технічно підкованих професіоналів і підприємців, представляючи унікальну можливість для маркетингу та охоплення.

Висновки. З розширенням технології блокчейн в сферах, відмінних від криптовалют, дослідницькі зусилля радикально розширилися протягом останніх років. Технологія блокчейн вважається революційним підходом у сфері державних послуг та електронного урядування та дає можливість громадянам, підприємствам та урядам легко взаємодіяти один з одним у прозорий спосіб. Її інноваційність походить від поєднання прозорості, цілісності, конфіденційності та підзвітності, якщо вона чітко розроблена. Крім того, розподілена блокчейн-мережа підвищує довіру між усіма учасниками, оскільки транзакції виконуються безпечно без схвалення центрального органу.

Література

1. A Survey on Blockchain for Information Systems Management and Security / D. Berdik та ін. Information Processing & Management. 2021. Т. 58, № 1. С. 102397. URL: https://doi.org/10.1016/j.ipm.2020.102397

2. Балацька , В., & Опірський, І. (2023). Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *4*(20), 6–19. https://doi.org/10.28925/2663-4023.2023.20.619

3. Балацька В.С., Опірський І.Р. механізми досягнення надійності в блокчейні для захисту персональних данихю Захист інформації і безпека інформаційних систем: матеріали IX Міжнар. наук.-техн. конф. – Львів : Видавництво Львівської політехніки, 2023. С. 17-18.

УДК 004.6

ІНТЕЛЕКТУАЛЬНА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОБРОБКИ ТА АНАЛІЗУ ДАНИХ ПОКУПЦІВ E-COMMERCE ДОДАТКІВ

Беккер Д.О., Марченко А.В.
Сумський державний університет, м. Суми

В публікації автори підкреслюють значення інтелектуального аналізу даних у електронній комерції для аналізу клієнтської поведінки та оптимізації бізнес-процесів. Результати досліджень даних відкривають шляхи для розробки цільових пропозицій, забезпечуючи стратегічне вдосконалення рекомендацій та логістики.

Ключові слова: наука про дані, інтелектуальний аналіз даних, електронна комерція, поведінка клієнта, машинне навчання.

In the publication, the authors emphasize the importance of data mining in e-commerce to analyze customer behavior and optimize business processes. The results of data research open the way for the development of targeted offers, ensuring strategic improvement of recommendations and logistics.

Keywords: data science, data mining, e-commerce, customer behavior, machine learning.

У динамічній сфері електронної комерції інтелектуальні інформаційні технології (ІІТ) відіграють вирішальну роль щодо вилучення стратегічної інформації з даних про клієнтів. Використовуючи широкий перелік методів: від аналізу даних до машинного навчання, компанії можуть адаптувати пропозиції, покращувати користувацький досвід і підвищувати операційну ефективність. Сила ІІТ полягає у перетворенні великих, складних наборів даних на дієву інформацію, що сприяє формуванню конкурентних переваг та стає джерелом інновацій в сфері e-commerce [1,2].

Автори дослідження заглиблюються в застосування інтелектуального аналізу даних про клієнтів, починаючи від очищення даних і статистичного аналізу і завершуючи побудовою моделей і алгоритмічних розвідок для важливих відкриттів [3,4]. Через застосування статистичного аналізу та технік дата майнингу було доповнено набір даних для побудови моделей прогнозування та сегментації клієнтів. Було проаналізовано дані, виявлено групи та кластери і побудовано вище згадані моделі. Використання цих моделей надає змогу бізнесу зрозуміти поведінку клієнтів та покращити продажі за рахунок спеціалізованих пропозицій дослідженим сегментам клієнтів. Також це удосконалює процес закупівлі товарів та оптимізації запасів, що підтверджується в роботах [5,6].

Початковий великий, але простий, набір даних перетворюється на більш змістовний і практичний актив з використанням інтелектуального аналізу для виявлення закономірностей і кластерів. За допомогою ітеративної клас-

теризації та групування відбувається збагачення базового набору даних. Такий підхід є прикладом доповнення даних, систематичного підвищення цінності та актуальності набору даних за допомогою розширеної, але доступної аналітики, що перетворює прості дані на всеосяжну бізнес-аналітику [7].

Збагачення спрямоване на розробку прогнозних моделей з використанням таких методів, як k-найближчих сусідів, дерев рішень і машин опорних векторів, а також на підвищення точності моделей за допомогою більш надійного набору даних [8].

Технологічна основа дослідження базується на Python, доповнена такими бібліотеками, як Pandas для обробки даних, Seaborn і Matplotlib для візуалізації, NumPy для числових задач, Scikit-learn для машинного навчання, SciPy для наукових розрахунків та Jupyter Notebook для інтерактивної розробки [9].

Розгортання складного інтелектуального аналізу даних у цьому дослідженні дозволить платформі електронної комерції отримати глибшу інформацію із комплексних наборів даних. В результаті, розроблене рішення можна впроваджувати в роботу бізнесу для оптимізації логістики та покращення стратегій продажів.

Література

1. Data Analytics in E-Commerce Retail. Режим допуску: https://towardsdatascience.com/data-analytics-in-e-commerce-retail-7ea42b561c2f

2. Machine Learning through the lens of e-commerce initiatives: An up-to-date systematic literature review. Режим допуску: https://www.sciencedirect.com/science/article/abs/pii/S157401372100054X?

3. Unlocking the Power of Data Science in eCommerce: A Comprehensive Guide. Режим допуску: https://www.orientsoftware.com/blog/data-science-in-ecommerce/#:~:text=Data%20science%20plays%20a%20crucial,goals%20and%20

4. E-commerce customer churn preservation using machine learning-based business intelligence strategy. Режим допуску: https://www.sciencedirect.com/science/article/pii/S2665917423000648?via%3Dihub

5. Research on E-Commerce Database Marketing Based on Machine Learning Algorithm. Режим допуску: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9259266

6. What are the most promising applications of data mining in e-commerce. Режим допуску: https://www.linkedin.com/advice/3/what-most-promising-applications-data-mining-e-commerce-waaye#:~:text=Data%20mining%20is%20the%

7. Data Mining. Режим допуску: https://golocad.com/glossary/data-mining/#:~:text=Data%20mining%20in%20e,reduce%20costs%20and%20maximize

8. A Data Mining Approach to Predict E-Commerce Customer Behavior. Режим допуску: https://link.springer.com/chapter/10.1007/978-3-319-92267-6_

9. Analysis of e-commerce customers' data mining based on Apriori optimization algorithm. Режим допуску: https://ieeexplore.ieee.org/document/10070248

УДК 004.8

РОЛЬ PYTORCH У РОЗВИТКУ СИСТЕМ ПОЖЕЖНОЇ БЕЗПЕКИ: ІННОВАЦІЇ ТА ЗАСТОСУВАННЯ

Беседа Андрій, Орлова Дар'я
Львівський державний університет безпеки життєдіяльності

Анотація. У даній тезі розглядається роль фреймворку PyTorch у розвитку систем пожежної безпеки, з акцентом на інноваційні підходи та практичне застосування. PyTorch, як гнучкий інструмент для машинного навчання, знайшов широке застосування у різних наукових та практичних сферах. Основна увага у тезі приділяється застосуванню згорткових нейронних мереж (CNN), які є ключовим елементом для класифікації зображень, розпізнавання об'єктів та мови. Описується процес обробки даних за допомогою CNN, починаючи від первинного аналізу простих особливостей, таких як лінії та кути, і закінчуючи розпізнаванням складних текстур та частин об'єктів. Особливий акцент робиться на можливості застосування PyTorch та CNN у контексті пожежної безпеки, включаючи розпізнавання диму та вогню на зображеннях або відео, створення симуляцій пожеж та розроблення тренувальних програм з використанням віртуальної реальності. Теза підкреслює значення PyTorch як інструменту, що сприяє розвитку ефективних та інноваційних рішень у сфері пожежної безпеки.

Ключові слова: фреймворк, PyTorch, згорткова нейронна мережа, пожежна безпека, класифікація.

PyTorch – це відкритий програмний пакет (фреймворк) для машинного навчання, який широко використовується в наукових дослідженнях та розробці. Розроблений на базі бібліотеки Torch, PyTorch пропонує гнучку та інтуїтивно зрозумілу платформу для створення та тренування нейронних мереж.[1] Основні особливості PyTorch:

– динамічне створення графів: надає змогу гнучко модифікувати та оптимізувати моделі нейронних мереж в процесі їх роботи.

– інтуїтивний Інтерфейс: чистий та зрозумілий API на основі Python, доступний для початківців

– сумісність з NumPy: легка інтеграція з NumPy для маніпуляції даними.

– підтримка CUDA: прискорення тренування моделей завдяки підтримці GPU.

Згорткова нейронна мережа (CNN) є ключовим інструментом для визначення та класифікації об'єктів, розпізнавання осіб на фото, аналізу мовлення та іншого. Згорткова нейронна мережа ефективно працює з різними типами даних, включаючи інформацію з датчиків, аудіо, відео та зо-

бражень. Унікальна властивість цієї мережі полягає у використанні операцій згортки, яка забезпечує одночасне зменшення обсягу збережених даних та виокремлення ключових характеристик зображення, таких як лінії, контури або кути. На наступних етапах обробки, мережа може ідентифікувати повторювані текстурні елементи, які потім збираються у більш складні фрагменти зображення.

В кожному шарі згорткової нейронної мережі використовується унікальне перетворення. Початкові шари фокусуються на простих особливостях, таких як лінії або кути, тоді як більш глибокі шари концентруються на більш складних елементах, таких як текстури та частини об'єктів. Це послідовне перетворення дозволяє точно класифікувати зображення або виокремлювати на завершальному етапі конкретні об'єкти на зображенні. [2].

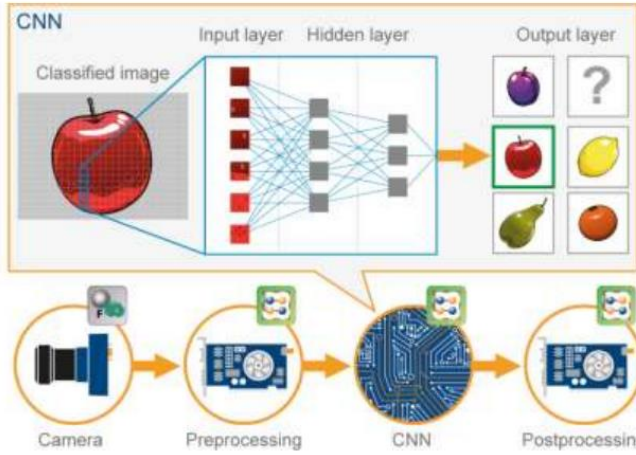


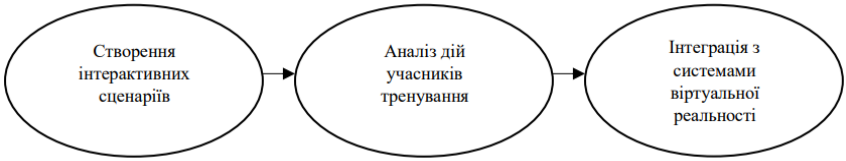
Рисунок 1 – Приклад класифікації зображення згортковою (CNN-мережею)

Використання PyTorch та згорткової нейронної мережі у контексті пожежної безпеки може включати різноманітні застсоування, а саме:

1. Розпізнавання диму та вогню на зображення чи відео для раннього виявлення пожеж у будівлях або на відкритих територіях:

2. Створення симуляції пожежі для моделювання різних сценаріїв пожеж для аналізу ефективності стратегії з гасінням пожежі:

3. Розроблення тренувальних симуляцій за допомогою віртуальної реальності.



Література

1. Електронний ресурс https://pytorch.org/docs/stable/index.html#
2. Електронний ресурс https://evergreens.com.ua/ua/articles/cnn.html

УДК 378.1

ДИСТАНЦІЙНЕ НАВЧАННЯ В УМОВАХ ВОЄННОГО СТАНУ

Бойко Оксана
Інститут державного управління та наукових досліджень з цивільного захисту

Анотація. В умовах воєнного стану особливого значення набуло дистанційне навчання, яке пройшло етап свого становлення під час пандемії. Перспективними є питання впровадження нових інформаційних технологій в освітньому процесі, подальшого вдосконалення дистанційних форм та методів навчання, наявності потрібного освітнього контенту на порталі закладу вищого освіти. Актуальним залишається проведення наукових досліджень на напрямі дистанційного навчання.

Ключові слова: освітній процес, дистанційне навчання, інформаційні технології, інноваційні методи навчання, воєнний стан

Abstract. In the conditions of martial law, remote learning, which has passed the stage of its formation during the pandemic, has acquired special importance. Prospective issues include the introduction of new information technologies in the educational process, further improvement of distance forms and methods of learning, and the availability of the necessary educational content on the portal of a higher education institution. Conducting scientific research in the field of distance learning remains relevant.

Key words: educational process, distance learning, information technologies, innovative methods of learning, martial law

З введенням в Україні 24 лютого 2022 року воєнного стану дистанційне навчання стало єдиною доступною та надійною формою в системі освіти. Відповідно до статті 57 Закону України «Про вищу освіту» щодо державних гарантій в умовах воєнного стану, надзвичайної ситуації або надзвичайного стану, зазначено, що здобувачам освіти, які в умовах воєнного стану, надзвичайної ситуації або надзвичайного стану в Україні чи окремих її місцевостях, оголошених у встановленому порядку (особливий період) були вимушені змінити місце проживання (перебування), залишити робоче місце, місце навчання, незалежно від їх місця проживання (перебування) на час особливого періоду гарантується організація освітнього процесу в дистанційній формі або в будь-якій іншій формі, що є найбільш безпечною для його учасників [1].

Дистанційне навчання є однією із форм навчання, яка виникла й удосконалювалася разом із розвитком інтернет-технологій, і тому має характерні ознаки, особливості, принципи і відповідні методичні напрацювання. Закономірно також, що дефініція «дистанційне навчання» має цілий ряд тлумачень. Використаємо визначення, наведене в наказі МОН від 08.09.2020 № 1115: «дистанційне навчання – організація навчального процесу (за дистанційною формою здобуття освіти або шляхом використання технологій дис-

танційного навчання в різних формах здобуття освіти) в умовах віддаленості один від одного його учасників та їх як правило опосередкованої взаємодії в освітньому середовищі, яке функціонує на базі сучасних освітніх, інформаційно-комунікаційних (цифрових) технологій. Водночас загалом аналогічно трактується це поняття і у Європейському Союзі (Резолюція 2001).

Успішній реалізації дистанційного навчання сприяє прийняття та реалізація Державної національної програми «Освіта» («Україна XXI століття»), Закону України «Про Національну програму інформатизації», Концепції розвитку дистанційної освіти в Україні та Положення про дистанційне навчання, затвердженого наказом МОН від 25.04.2013 № 466 (зі змінами), інших нормативно-правових актів.

Актуальні питання організації дистанційного навчання в умовах воєнного стану досліджували О. Гнатюк, І. Діордіца, Д. Зварич, О. Кошелєва, Н. Куриш, Ю. Лахмотова, М. Мар'єнко, Н. Мезенцова, А. Мельник, Н. Родіонова, А. Сухіх, С. Толочко, В. Троцько, М. Червоній, І. Чернозубкін, М. Яненко та інші.

А. Мельник досліджує проблеми використання елементів дистанційного навчання в умовах воєнного стану, зокрема особливості й технологічні переваги дистанційного навчання, його слабкі сторони, які можна нівелювати за рахунок активного використання моделей змішаного навчання [2].

В. Троцько та І. Чернозубкін у своєму дослідженні аналізують накопичений досвід використання системи дистанційного навчання в умовах воєнного стану, зокрема названо ознаки сталого функціонування системи дистанційного навчання: відсутність постійної безпосередньої загрози життю та здоров'ю всіх користувачів системи; відсутність технічних збоїв внаслідок воєнних дій; наявність надійної комунікації електронними засобами для користувачів системи; можливість для розвитку системи дистанційного навчання [3].

Інноваційні методи навчання та викладання, питання інноваційних методик навчання та проблемно-орієнтованого навчання, використання мультимедіа-технологій у навчальному процесі, елементи проблемно-орієнтованого навчання, а також методологічне забезпечення розробки ситуаційного завдання за методом кейсів розглянуто у навчальному посібнику, авторами якого є П. Волянський, О. Євсюков, В. Михайлов, А. Терент'єва та К. Шихненко [4].

В умовах воєнного стану суттєво зростає роль функціонального навчання (підвищення кваліфікації цільового призначення) керівного складу та фахівців, діяльність яких пов'язана з організацією і здійсненням заходів з питань цивільного захисту, яке здійснюють Інститут державного управління та наукових досліджень з цивільного захисту (для центральних органів виконавчої влади та інших органів державної влади) і навчально-методичні центри цивільного захисту та безпеки життєдіяльності в регіонах (для місцевих органів виконавчої влади, органів місцевого самоврядування, територіальних формувань цивільного захисту та суб'єктів господа-

рювання незалежно від форм власності). В умовах воєнного стану функціональне навчання здійснюється у дистанційній формі з використанням програми ZOOM та платформи MOODLE. Лише впродовж 2022 року, в умовах воєнного стану, зазначене навчання на базі навчально-методичних центрів цивільного захисту та безпеки життєдіяльності в регіонах пройшли 35 тисяч 73 особи керівного складу та фахівців [5, с. 10].

Дистанційне навчання передбачає обов'язковий доступ до інтернету, технічне забезпечення (комп'ютер, ноутбук, планшет, смартфон тощо).

Сучасний рівень комп'ютерної техніки та різноманітного програмного забезпечення надає широкі можливості для підвищення ефективності навчання, але в умовах воєнного стану використання комп'ютерних технологій значно ускладнюється відключеннями електроенергії внаслідок ворожих обстрілів об'єктів енергетики, обов'язковою стає наявність резервних електрогенераторів тощо.

Глобальна інформатизація сучасного суспільства, розвиток телекомунікаційних, комп'ютерних та інформаційних технологій – з одного боку, та триваюча російсько-українська війна – з другого, обумовлюють кардинальні зміни пріоритетних форм здійснення освітнього процесу; і дистанційне навчання в цих умовах стає найперспективнішим варіантом надання якісних освітніх послуг при мінімальних витратах коштів на його організацію. Слід також врахувати те, що МОН ініціює внесення до Верховної Ради України урядового законопроєкту щодо скасування заочної форми навчання вже з наступного 2024 року та заміни дистанційною формою і так званою індивідуальною траєкторією, як гнучкою формою денного навчання.

Література

1. Про вищу освіту. Закон України «Про освіту» від 05.09.2017 р. № 2145 – VIII. Дата оновлення: 07.02.2023. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text (дата звернення: 16.11.2023).

2. Мельник А.І. Проблеми використання елементів дистанційного навчання в умовах воєнного стану. *Вісник КНЛУ. Серія Педагогіка та психологія.* 2022. Випуск 37. С. 64 – 75.

3. Троцько В., Чернозубкін І. Досвід використання системи дистанційного навчання в умовах воєнного стану. *Вчені записки Університету «КРОК».* 2023. № 2 (70). С. 64 – 75.

4. Організація та проведення занять із застосуванням інноваційних методів: навчальний посібник/Укладачі: Волянський П.Б., Євсюков О.П., Михайлов В.М., Терент'єва А.В., Шихненко К.І. Київ: ІДУ НД ЦЗ, 2022. 131 с.

5. Публічний звіт про основні результати діяльності Державної служби України з надзвичайних ситуацій у 2022 році. URL: https://dsns.gov.ua/upload/1/6/4/9/3/5/0/publicnii-zvit-2022-ostannia-versiia-1.pdf (дата звернення: 16.11.2023).

УДК 614.842

АНАЛІЗ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ З МЕТОЮ ПІДТРИМКИ РІШЕНЬ В ПРОЦЕСІ ОПЕРАТИВНОГО РЕАГУВАННЯ ПІДРОЗДІЛІВ ДСНС УКРАЇНИ

Босак Г., Головатий Р.
Львівський державний університет безпеки життєдіяльності

Сучасні досягнення інформаційних технологій реалізації систем керування різними типами об'єктів і процесів пов'язані з широким впровадженням у практику впровадження інформаційно-керуючих систем моделей та методів, а також спеціальних засобів програмування, регламентовані міжнародними стандартами, а також впровадження сучасних основ побудови інформаційних систем управління. На сьогодні рятувальні підрозділи ДСНС України є надзвичайно важливою структурую, оскільки рятувальні служби виконують ключову роль у збереженні життя та майна під час надзвичайних ситуацій, особливо внаслідок обстрілів житлової інфраструктуру окупантами. Інформаційно-керуючі системи стали невід'ємною частиною роботи цих підрозділів, допомагаючи вдосконалити координацію та ефективність їх дій. На діяльність рятувального підрозділу значною мірою впливає швидкість, з якою дані про хід ліквідації надзвичайних ситуацій можуть бути отримані, оброблені та передані. Інформаційні технології в системі ДСНС України спрямовані на вдосконалення діяльності оперативних служб шляхом процесів управління, вирішення завдань із забезпечення пожежної, техногенної та цивільної безпеки.

Ключові слова: інформаційні технології, підрозділи ДСНС України, оперативне управління.

Modern achievements of information technologies for the implementation of management systems of various types of objects and processes are associated with the wide implementation in the practice of information management systems of models and methods, as well as special programming tools regulated by international standards, as well as the implementation of modern foundations for the construction of information management systems . Today, rescue units of the State Emergency Service of Ukraine are an extremely important structure, as rescue services play a key role in saving life and property during emergency situations, especially as a result of shelling of residential infrastructure by occupiers. Information and management systems have become an integral part of the work of these units, helping to improve the coordination and efficiency of their actions. The speed with which emergency response data can be received, processed, and transmitted is greatly influenced by the speed with which emergency response data can be received, processed, and transmitted. Information technologies in the system of the State Emergency Service of Ukraine are aimed at improving the operations of operational services through management processes, solving tasks to ensure fire, man-made and civil safety.

***Keywords*:** information technologies, divisions of the State Emergency Service of Ukraine, operational management.

Швидкість ескалації соціально-політичної ситуації та масштаби можливих негативних наслідків вимагають створення нових, відповідних рівню загроз, нормативно-правових та організаційних механізмів для підтримки процесів ухвалення та формування рішень щодо попередження, реагування та ліквідації наслідків надзвичайних ситуацій воєнного, техногенного, природного та соціально-політичного характеру.

Очевидно, що у важкий час, в якій нині перебуває Українська держава, яка відстоює свою цілісність та Державний суверенітет, тільки підкреслює необхідність створення спеціалізованої організаційної структури в системі забезпечення національної безпеки – ситуаційного центру. Він має за мету забезпечення підтримки прийняття рішень з реалізації заходів на всіх етапах управління надзвичайними ситуаціями [4]. Аналіз інформаційних технологій для підтримки рішень в процесі оперативного реагування підрозділів ДСНС України включає в себе розгляд різноманітних аспектів, таких як системи збору та обробки інформації, комунікаційні технології, аналітичні засоби та програмне забезпечення для прийняття ефективних рішень в екстрених ситуаціях [3].

Основні компоненти такого аналізу можуть включати:

1.*Системи моніторингу та збору інформації*:

- сенсорні системи: використання сучасних сенсорів (наприклад, вимірювачів температури, давлення, атмосферного тиску) для отримання реального часу даних про обстановку.
- системи відеоспостереження: розгортання відеокамер для візуального контролю за територією та вчасного реагування на події.
- системи дистанційного зондування: використання супутникових та аерозйомних систем для збору геопросторової інформації.

2.*Системи комунікації*:

- мобільні технології: забезпечення підрозділів засобами мобільного зв'язку та обміну даними для оперативного спілкування.
- системи радіочастотного зв'язку: забезпечення ефективного радіозв'язку для забезпечення комунікації в областях з обмеженим доступом.

3.*Аналітичні інструменти*:

- системи обробки даних в реальному часі: використання потужних аналітичних інструментів для швидкої обробки та аналізу великих обсягів даних.
- геоінформаційні системи (ГІС): використання ГІС для візуалізації геопросторової інформації та планування дій.

4.*Системи управління ресурсами*:

- системи розподілу задач: автоматизація процесів розподілу завдань та координації дій між різними підрозділами.
- системи управління персоналом: забезпечення ефективного управління персоналом та розподілом ресурсів.

5.*Тренування та симуляції*:

– системи віртуального тренування: використання віртуальних середовищ для тренувань та симуляцій екстрених ситуацій.

6.*Кібербезпека*:

– системи кіберзахисту: захист інформаційних систем від кібератак та забезпечення цілісності та конфіденційності даних.

Цей аналіз має на меті визначити найбільш ефективні та інтегровані технологічні рішення для підтримки оперативного реагування підрозділів ДСНС України та покращення їхньої загальної ефективності. Також важливо враховувати фактори масштабування та можливість адаптації до змінних умов екстрених ситуацій [2].

Для подолання надзвичайних ситуацій (особливо внаслідок ракетних обстрілів окупантами) необхідно подальше вдосконалення системи забезпечення національної безпеки України [1]. Це передбачає підвищення ефективності механізмів формування та підтримки прийняття рішень в галузі попередження, реагування та ліквідації наслідків надзвичайних ситуацій різного характеру, такого як воєнного, техногенного, природного та соціально-політичного.

Література

1. Безугла К. О. Сучасний стан сектору інформаційних технологій в Україні. Економіко-математичне моделювання соціально-економічних систем. Збірник наукових праць. Випуск 19. К.: МННЦ ІТіС, 2014. С. 50-70

2. Бурак Н. Є. Модель проектно-інформаційного середовища покращення підготовки рятувальника в ментальному просторі ІТ-технологій. Вісник Львівського державного університету безпеки життєдіяльності. Львів, 2014. № 10. С. 24-32.

3. Кузьомін О. Я. Методи, моделі та інформаційні технології моніторингу і ліквідації наслідків надзвичайних природних ситуацій: автореф. дис.. д-ра техн. наук: 05.13.06. Харківський національний ун-т радіоелектроніки. Х., 2008. 31 с.

4. Нестеренко О., Поліщук В., Хижняк В., Шевченко В. Інформаційні технології підтримки прийняття рішень щодо визначення ресурсів для гасіння лісової пожежі засобами авіації. Екологічна безпека та природокористування, 46(2), 2023. С. 109–123.

УДК 004.71

АНАЛІЗ РЕАЛІЗАЦІЇ ПРОТОКОЛУ ДИНАМІЧНОЇ КОНФІГУРАЦІЇ ВУЗЛІВ

Василюк Владислав, Бурак Назарій
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі розглянуто важливість мережевих протоколів у структурі мереж та їхню роль у забезпеченні ефективного обміну інформацією в цифровому світі. Проаналізовано реалізацію мережевого протоколу DHCP, зокрема досліджено процес ініціалізації та передачі параметрів автоматичної конфігурації клієнтів.

Ключові слова: комп'ютерна мережі, протокол, хост, взаємодія

The paper considers the importance of network protocols in the structure of networks and their role in ensuring effective information exchange in the digital world. The implementation of the network protocol DHCP was analysed. Explored the initialization and transfer process of client automatic configuration.

Keywords: computer network, protocol, host, interaction

Мережеві протоколи відіграють визначальну роль у структурі та функціонуванні сучасних мереж, будуючи невидимий каркас, що дозволяє пристроям взаємодіяти та обмінюватися інформацією. Подібно до того, як спілкування однією мовою спрощує спілкування між двома людьми, мережеві протоколи дають змогу пристроям взаємодіяти один з одним завдяки заздалегідь визначеним правилам, вбудованим у програмне та апаратне забезпечення пристроїв. Без протоколів пристрої не змогли б зрозуміти електронні сигнали, що передаються між ними через мережеві з'єднання. Ні локальні мережі (LAN), ні глобальні мережі (WAN) не могли б функціонувати так, як вони працюють сьогодні, без використання мережевих протоколів.

Мережевий протокол — це встановлений набір правил, які визначають спосіб передачі даних між різними пристроями в одній мережі. Застосування таких правил дозволяє підключеним пристроям спілкуватися один з одним, незалежно від будь-яких відмінностей у їхніх внутрішніх процесах, структурі чи дизайні.

Під час передачі даних мережею, вони діляться на невеликі біти, які називаються пакетами. Кожне велике повідомлення, що передається між двома мережевими пристроями, часто ділиться на менші пакети, щоб підвищити продуктивність і стабільність мережі. Кожен пакет складається з трьох основних частин: заголовка, корисного навантаження та нижнього колонтитула. Мережі потрібна контекстна інформація, наприклад адреси пристроїв надсилання та отримання, які містяться в заголовках і нижніх

колонтитулах пакетів. Таку інформацію про вузли забезпечує протокол динамічної конфігурації вузлів, який часто використовують у сучасних мережах при адресації.

Протокол динамічної конфігурації хоста (Dynamic Host Configuration Protocol –DHCP) - це протокол, який використовується пристроями, підключеними до мережі, для розподілу та використання IP-адрес.

Інтерфейс протоколу DHCP між сервером і клієнтом автоматично призначає адресу та інші дані хосту, що дає змогу кінцевому пристрою отримувати від сервера усю необхідну інформацію про конфігурацію протоколу керування передачею (TCP/IP). Отримання адреси та інших параметрів є життєво важливим компонентом, який необхідно призначити всім пристроям для злагодженої взаємодії.

Основним компонентами мережі, реалізованої на основі протоколу DHCP є сервер, клієнти та підмережі. Інколи також присутні ретранслятори, роль який виконую маршрутизатори, які діють як посередники між клієнтами та сервером, посилюючи повідомлення для досягнення мети призначення.

Загальний процес роботи протоколу наведений на рисунку 1.

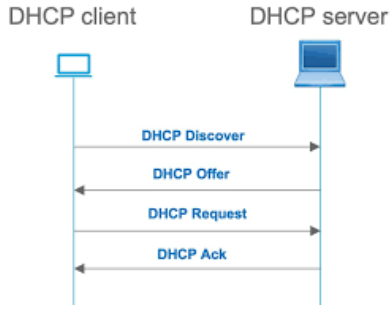


Рисунок 1 – Принцип роботи протоколу DHCP

Щоб отримати IP-адресу, клієнтський пристрій надсилає широкомовне повідомлення — DHCPDISCOVER для виявлення сервера DHCP, який функціонує в мережі. Функції DHCP-сервера зазвичай призначаються фізичному серверу та резервному. Інші пристрої також можуть діяти як сервери DHCP, наприклад бездротові точки доступу. Після отримання повідомлення DHCPDISCOVER, DHCP-сервер резервує IP-адресу для клієнта, що підключається, та інші параметри конфігурації мережі, включаючи шлюз за замовчуванням із маскою підмережі, бажаний DNS-сервер, і надає доступ до неї клієнтському пристрою через повідомлення DHCPOFFER. Клієнт відповідає на пакет DHCPOFFER сервера за допомогою повідомлення DHCPREQUEST із запитом запропонованої IP-адреси та відповідної конфігурації мережі, на-

дісланої сервером DHCP для системи. Отримавши повідомлення із запитом від клієнта, сервер підтверджує широкомовну передачу DHCPREQUEST від клієнтського пристрою та надсилає клієнту DHCP пакет DHCPACK, який містить необхідну конфігурацію мережі для клієнтського пристрою.

Все це робиться швидко й автоматично, і кінцевому користувачеві не потрібно виконувати жодних дій. Сервер відстежує використання адреси та повертає її у загальнодоступний пул через визначений час або коли пристрій вимикається і може бути перепризначена іншому пристрою.

Завдяки взаємодії мережевих протоколів та DHCP, створюється динамічна система, яка самостійно адаптується до змін у складі пристроїв, що підключаються до мережі. Це робить мережі більш гнучкими та легкими у впровадженні, зменшуючи трудомісткість та забезпечуючи миттєвий доступ до ресурсів.

Література

1. Dooley, Michael & Rooney, Timothy. (2020). DHCP Reference. DOI:10.1002/9781119692263.ch18.

2. Герговський О., Бурак Н.Є. Аналіз функціональних особливостей комутаторів Layer 2 та Layer 3. Інформаційна безпека та інформаційні технології ІБІТ-2022: збірних тез доповідей IV Міжнародної науково-практичної конференції, 30 листопада 2022 року. – Львів, ЛДУ БЖД, 2022. – С.199-201

3. Panek, William. (2018). Configuring DHCP. DOI:10.1002/9781119549260.ch12.

4. Parulkar, Amey. (2021). DHCP and DNS.

УДК 519.83

АНАЛІЗ БАГАТОКРИТЕРІАЛЬНИХ МЕТОДІВ ВИБОРУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Величко Софія, Зінов'єва Ольга
Таврійський державний агротехнологічний університет імені Дмитра Моторного

Анотація – В роботі розглядаються методи багатокритеріального вибору альтернативи для прийняття рішення.
***Ключові слова*:** багатокритеріальний вибір, альтернатива, метод багатокритеріальної теорії корисності, метод аналізу ієрархій.

Summary – The work considers the methods of multi-criteria selection of an alternative for decision-making
***Keywords*:** multi-criteria choice, alternative, method of multi-criteria theory of utility, method of analysis of hierarchies

Застосування програмного забезпечення в високотехнічних сферах промисловості визначає висока вимоги до якості і надійності програмних засобів. Велика кількість версій програмних пакетів становлять перед проектувальником задачу прийняття рішення по вибору програмного забезпечення з урахуванням ряду критеріїв. Оскільки вибор оптимального варіанту програмного забезпечення представляє собою задачу вибору з множини альтернатив, то доцільно використовувати методи багатокритеріального вибору прийняття рішень.

Для таких задач, як отримання критеріальних оцінок альтернатив, моделювання переваг особи, яка приймає рішення, вибір оптимального рішення існують досить добре опрацьовані на теперішній час підходи до їх моделювання. В даній роботі розглядаються три найбільш широко відомих методи – методи багатокритеріальної теорії корисності (MAUT) , аналітичної ієрархії (MAI), відношення переваги по якості (ELECTRE).

Існують різні методи до розв'язання задач вибору найбільш переважного варіанту. Серед тих, що найбільше використовуються:

- методи, що базуються на кількісних вимірюваннях (багатокритеріальна теорія корисності MAUT);
- методи, які основані на якісних вимірюваннях, результати яких переводяться в кількісний вигляд (метод аналізу ієрархій);
- методи, які основані на якісних вимірюваннях, але використовують декілька показників при порівнюванні альтернатив (методи Electre)/

На лабораторних заняттях студенти знайомляться з методами MAUT та методом аналізу ієрархій. Ми зробимо порівняльний аналіз методів для розв'язання задачі вибору програмного пакету як задачі прийняття рішення.

Задача полягає у виборі найкращої альтернативи серед трьох програмних проектів за 8 критеріями (математичне забезпечення, функціональність, інтерфейс, складність побудови і т.д.).

За методом багатокритеріальної теорії корисності MAUT (Multi-Attribute Utility Theory):

1) будується функція корисності;
2) деякі умови, які визначають форму цієї кривої, належать перевірці в діалозі з особою, яка приймає рішення;
3) отримані результати використовують для оцінки заданих альтернатив.

Теорія корисності базується на загальних аксіомах та аксіомах незалежності. При виконанні умови строгої незалежності, функція корисності має або адитивний, або мультиплікативний вигляд

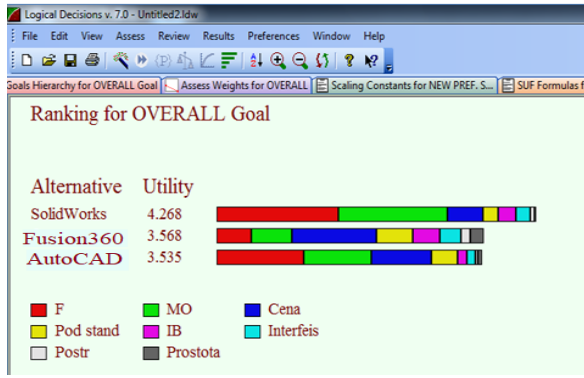


Рисунок 1 – Результат роботи програми Logical Decisions

Переваги метода: за допомогою метода MAUT можна визначити корисність кожної альтернативи, хоча побудова загальної функції корисності потребує багато часу та зусиль особи, яка приймає рішення, отриманий результат дозволяє оцінити будь-які альтернативи.

До недоліків методу можна віднести те, що особа, яка приймає рішення, повинна спочатку задати точні кількісні визначення всіх основних параметрів, що є досить складним.

Метод аналізу ієрархій дозволяє розв'язувати задачу багатокритеріального вибору слабоформалізованих альтернатив.

Метод полягає в декомпозиції проблеми на більш прості складові частини та подальшій обробці суджень по парним порівнянням. Ці судження потім виражаються кількісно.

Метод MAI складається з наступних етапів:

1) перший етап полягає в структуризації задачі у вигляді ієрархічної структури: мети – критерії – альтернативи
2) На другому етапі особа, яка приймає рішення виконує попарні порівняння елементів кожного рівня. Результати порівнянь переводяться в числа.
3) Обчислюються коефіцієнти вагомості для елементів кожного рівня. Перевіряється погодженість суджень експертів.
4) Підраховуються вектори глобальних пріоритетів і визначається найкраща альтернатива

Перевагою методу MAI є спрямованість цього методу на порівняння реальних альтернатив.

До недоліків можна віднести те, що введення нової альтернативи може привести до зміни переваг між двома раніш заданими альтернативами.

Методи ELECTRE спрямовані на розв'язання задач з вже заданими ба-гатокритеріальними альтернативами. На відміну від метода MAI в методах ELECTRE не визначається кількісно показник якості кожної з альтернатив, а встановлюється лише умова переваги однієї альтернативи над іншою.

Важливою перевагою методів ELECTRE є поетапність виявлення пере-ваг особи, яка приймає рішення в процесі визначення рівнів згоди і незгоди та вивчення ядер.

Кожний з розглянутих методів досить поширено використовується в комп'ютерних системах підтримки рішень (метод MAUT в системі Logical Decisions, метод MAI – в СППР "Decisioner", EXPERT CHOICE, метод ELECTRE – в системі ELECTRE III. Складності можуть виникати при назначенні особою, яка приймає рішення, вагів

Література

1. Гнатієнко Г. М. Експертні технології прийняття рішень / Г. М. Гнатієнко., В. Є. Снитюк. – Київ : ТОВ „Маклаут", 2008. – 444 с..

2. Нестеренко О.В. Інтелектуальні системи підтримки прийняття рішень: навч. посібн./ О.В. Нестеренко, О.І. Савенков, О.О. Фаловський. За ред. П.І. Бідюка. – Київ: Національна академія управління. – 2016. – 188 с.

3. Системи підтримки прийняття рішень : навч. посіб. / М.А. Демиденко; Нац. гірн. ун-т. -- Електрон. текст. дані. – Д. : 2016. – 104 с.

УДК 351.861

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ QUICK RESPONSE ДЛЯ ПОПЕРЕДЖЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКУТРИ В УМОВАХ ВПЛИВІВ ВОЄННОГО ЧАСУ

Вовчук Таїсія, Шевченко Ольга, Шевченко Роман
Національний університет цивільного захисту України, м. Харків

Розглянуто розв'язання завдання з розробки інформаційної технології аналітичної підтримки процесу попередження надзвичайних ситуацій техногенного характеру на об'єктах критичної інфраструктури в умовах впливів воєнного часу, з урахуванням сучасних можливостей технологій QR-кодування.

Ключові слова: інформаційні технології, об'єкти критичної інфраструктури, QR-кодування.

The solution to the task of developing information technology for analytical support of the process of preventing emergencies of man-made nature at critical infrastructure facilities under the conditions of wartime effects, taking into account the modern capabilities of QR-coding technologies, is considered.

Keywords: information technologies, critical infrastructure objects, QR-coding.

Аналіз стану техногенної та природної безпеки в Україні за умов негативних впливів воєнного стану доводить зростання кількості надзвичайних ситуацій (НС), як в цілому в державі, так і безпосередньо в зоні бойових дій. Одним із шляхів підвищення ефективності системи протидії НС є застосування сучасних інформаційних технологій, як у процесі прогнозування та моніторингу НС, так і під час їх локалізації та ліквідації. Для ефективного виконання останнього завдання необхідно органічно вирішити неоднозначну ситуацію, яка обумовлена наявним протиріччям між стрімким розвитком можливостей інформаційних технологій, з одного боку, та застарілими підходами щодо організації інформаційної підтримки дій аварійно-рятувальних підрозділів, з іншого.

Одним із шляхів вирішення зазначеного протиріччя є комплексне використання технології quick response (QR) - кодування та інноваційних експрес методів ідентифікації небезпеки в питаннях інформування особового складу аварійно-рятувальних підрозділів та населення щодо дій в умовах НС на об'єктах критичної інфраструктури.

У відповідності до основних положень програми інформатизації системи Міністерства внутрішніх справ України, автоматизація процесів підготовки сил та засобів до виконання завдань із ліквідації надзвичайних ситуацій, включає в себе:

1) планування застосування сил Національної поліції, Національної гвардії, Державної служби з надзвичайних ситуацій та інших органів системи МВС;

2) постановку завдань з ліквідації надзвичайних ситуацій;

3) збір, аналіз та інтеграцію оперативних даних зони виконання завдань;

4) оперативний обмін інформацією,

Такий поділ завдань дозволяє автоматизувати процес прийняття рішення щодо ефективного застосування об'єднаних сил і засобів у швидкозмінній обстановці впливі воєнного часу з метою попередження, локалізації та ліквідації надзвичайних ситуацій в першу чергу на об’єктах критичної інфраструктури.

Виходячи з наведеного автоматизована система QR-управління повинна включати в себе:

1) відображення загальної оперативної картини зони виконання завдань з геопросторовою прив’язкою, яка відображає в режимі реального часу розміщення сил та засобів, що залучаються до заходів з ліквідації надзвичайних ситуацій;

2) об'єднувати в собі дані з різноманітних джерел інформації;

3) мати можливість деталізації обстановки за допомогою відеосигналу, відображення координат місць знаходження аварійно-рятувальних підрозділів, спеціальних та транспортних засобів тощо;

4) мати можливість здійснювати динамічний контроль просторового положення сил, обмін стислими текстовими повідомленнями та забезпечувати відеотелефонний зв'язок керівника з ліквідації наслідків надзвичайної ситуації на об’єктах небезпечного виробництва з керівниками нижчих ланок на місцях виконання завдань;

5) мати доступ до системи диспетчерського (оперативного) радіозв'язку системи ДСНС та МВС в цілому, а у разі трансграничного поширення НС, мати доступ до систем країн партнерів.

Окремі можливості автоматизованої системи QR-управління надзвичайною ситуацією повинні забезпечити взаємодію з населенням, що прогнозновано може опинитися в зоні поширення надзвичайної ситуації на об’єкті критичної інфраструктури. Від так остання повинна бути інтегрована в Систему екстреної допомоги населенню за єдиним телефонним номером 112.

Така інтеграція повинна будуватися на принципах комплексного надання допомоги населенню у разі виникнення екстрених ситуацій, що загрожують здоров’ю, життю, майну або навколишньому природному середовищу, інших небезпечних та катастрофічних подій.

Базовими, у побудові взаємодії, мають бути наступні компоненти:

1) широке використання інформаційно-телекомунікаційних технологій, в першу чергу QR кодування та QR відтворення даних, при налаштуванні доступу населення до системи надання екстреної допомоги, а також організації електронної взаємодії нарівні суб’єктів, що забезпечують реагування на катастрофічну екстрену подію;

2) взаємодія та використання інформаційних (QR), інформаційно-телекомунікаційних систем МВС для інформаційно-аналітичної підтримки при прийнятті рішень під час реагування на екстрені та надзвичайні події;

3) використання засобів відеоспостереження та фіксації подій в реальному часі;

4) застосування електронних пристроїв та систем уповноваженими ЦОВВ та іншими органами виконавчої влади з метою попередження екстрених подій та оперативного реагування у разі їх виникнення.

Побудова відповідної взаємодії в межах автоматизованої системи QR-управління надзвичайною ситуацією шляхом сумісності традиційних методів реагування на катастрофічні події і інформаційно-телекомунікаційних технологій дозволить в рази підвищити ефективність надання допомоги населенню та значно удосконалити діяльність аварійно-рятувальних служб та інших служб, що залучаються, віддалено бачити ситуацію на місці екстреної події, оперативно задіяти доступні ресурси, забезпечувати інформацією урядові та регіональні кризові центри в реальному масштабі часу.

Ключовим моментом всієї координації є обмін інформацією. Пошук і порятунок людей при катастрофах і НС з великою кількістю постраждалих (витоки нафти й особливо небезпечних хімічних речовин, терористичні акти) складають 80% від всієї кількості випадків, тому ліквідація їх наслідків відбувається згідно заздалегідь розроблених принципів й алгоритмів. Решта випадків є комплексними, тобто з поєднанням специфіки декількох випадків одночасно.

Основним організаційним принципом взаємодії повинна бути система горизонтальних та вертикальних зв'язків різних рівнів реагування, що побудовані на єдиній інформаційно-аналітичній системі QR-управління надзвичайною ситуацією на об'єктах критичної інфраструктури.

Іншим основним принципом є уніфікація та стандартизація, з урахуванням вимог правового та інформаційно-аналітичного простору країн Європейської спільноти, заходів з попередження надзвичайною ситуацією техногенного характеру на об'єктах критичної інфраструктури, що дозволить забезпечити оптимальні умови для створення матеріальних резервів та підготовки кадрів аварійно-рятувальних підрозділів.

Висновки. Таким чином, зважаючи на орієнтацію України на європейські стандарти в сфері цивільного захисту, виникає потреба у необхідності узагальнення та імплементації міжнародного досвіду створення та функціонування систем управління в умовах надзвичайних ситуацій, на базі сучасних інформаційно-комунікативних технологій (на шталт QR-техно логій), з подальшим завданням щодо їх широкого застосування в системі попередження надзвичайних ситуацій різного характеру.

УДК 338.47

3D ДРУК ТА ЙОГО ЗАСТОСУВАННЯ В УПРАВЛІННІ ЛАНЦЮГОМ ПОСТАВОК

Воробей Артем, Товарянський Володимир
Львівський державний університет безпеки життєдіяльності, Львів

Описано важливість 3D друку умовах сьогодення. Наведено актуальні приклади застосування тривимірних технологій для функціональних областей логістики. Відзначено тенденції впровадження 3D технологій для логістики та вантажних перевезень. Відзначено, що особливої уваги заслуговують процеси складування продукції, оптимізувати які можливо з використанням 3D принтерів. Ключові слова: 3D друк, 3D принтер, управління ланцюгами поставок, виробництво.

The importance of 3D printing in today's conditions is described. Current examples of the application of three-dimensional technologies for functional areas of logistics are presented. Trends in the introduction of 3D technologies for logistics and freight transportation are noted. It was noted that the processes of storing products deserve special attention, which can be optimized using 3D printers. Keywords: 3D printing, 3D printer, supply chain management, manufacturing.

Найбільший потенціал 3D принтерів стосується здатності спрощувати виробничі, складські та транспортні процеси, оскільки їх оптимізація призводить до скорочення часу доставки [1].

В даний час на багатьох складах зберігаються значні обсяги сировини, яка своєчасно надходить на виробничі лінії. У разі здійснення 3D друку немає необхідності зберігати таку кількість ресурсів, оскільки елементи можна виготовити за необхідністю. 3D принтери можуть забезпечити швидке та безпечне виробництво всіх типів компонентів.

Від цього, безсумнівно, виграють автомобільна та авіаційна промисловість, оскільки для досягнення своїх цілей забезпечується «гнучка логістика» та «своєчасне виконання» завдань [2]. Специфіка діяльності даного сектору полягає в тісній співпраці з постачальниками, які повинні своєчасно постачати необхідні комплектуючі та матеріали.

Найважливіші переваги щодо ефективності використання 3D друку для ланцюгів поставок:

– обмеження запасів: виробництво на замовлення допомагає скоротити витрати на зберігання, оскільки лише вихідні матеріали та готові вироби зберігаються в очікуванні відправлення клієнту;

– використання простору: менше запасів становлять меншу потребу в складських приміщеннях;

– зменшення транспортних витрат: 3D принтери не вимагають багато місця, тому їх можна встановити на заводі, розташованому неподалік від головного офісу замовника.

Крім того, 3D принтери дозволяють персоналізувати продукт відповідно до потреб клієнтів. З точки зору логістики та управління ланцюгами поставок, найбільша складність полягає в забезпеченні ефективної обробки зростаючої кількості вантажів. Для цього необхідно налагодити систему для якісного складського управління, яка буде керувати процесами персоналізації та комплектації.

Немає сумнівів, що 3D друк принесе довгострокові зміни в логістиці. На додаток до очевидних переваг, які 3D друк може принести логістичній галузі, слід також взяти до уваги виклики, пов'язані з далекосяжними змінами в ланцюзі поставок багатьох підприємств. З одного боку, можна очікувати обмеження на транспортування деяких продуктів через можливість, наприклад, друкувати компоненти безпосередньо на виробничій лінії. З іншого боку, необхідно буде оперативно переміщувати витратні матеріали для принтерів.

Література

1. Manners-Bell, J., & Lyon, K. (2012). The implications of 3D printing for the global logistics industry. *Transport Intelligence*, 1–5.

2. Rutkowski K., Ocicka B. (2017). Rozwój druku 3D i jego wpływ na zarządzanie łańcuchem dostaw. Gospodarka Materiałowa i Logistyka. N. 12. – St. 2-11.

УДК 378.147

МОБІЛЬНЕ НАВЧАННЯ ЯК ІННОВАЦІЙНА ІНФОРМАЦІЙНО-КОМУНІКАТИВНА ТЕХНОЛОГІЯ

Гайович Галина
Інститут державного управління та наукових досліджень з цивільного захисту, м. Київ

У розвідці розглянуто мобільне навчання як одну з інноваційних інформаційних технологій у навчанні. Зазначено, що таке навчання розширює можливості активізації тих, хто навчається, та дозволяє проводити навчання в нестандартних умовах, зокрема й у ситуаціях, що виникають через війну. Зроблено висновок про позитивний вплив мобільних технологій на організацію навчального процесу.

Ключові слова: мобільне навчання, гаджет, мобільні технології, умови воєнного стану.

The article analyses mobile learning as one of the innovative information technologies in education. It is noted that such training mode expands the possibilities of activation of students and allows them to study in non-standard conditions, in particular, in situations arising due to war. A conclusion is made about the positive impact of mobile technologies on the educational process organization.

Keywords: mobile learning, gadgets, mobile technologies, martial law conditions.

В Україні активізується впровадження в освітній процес інформаційно-комунікаційних технологій, зокрема й тих, що забезпечують мобільне навчання (англ. m-learning). В умовах воєнного стану, оголошеного у зв'язку з військовою агресією Російської Федерації проти України [1], впровадження такого виду навчання в освітній процес є одним з перспективних.

Мобільне навчання ґрунтується на використанні гаджетів – невеликих електронних пристроїв [2]. Вони дозволяють виконувати різні дії, зокрема, надсилати повідомлення, створювати документи у форматі Word, фотографувати, слухати різний контент, підключатися до різних форматів онлайн-зустрічей, користуватися поштовою скринькою, спілкуватися в соціальних мережах тощо. Усе це не лише розширює можливості активізації тих, хто навчається, але й надає більше можливостей для проведення навчання в умовах воєнного стану, що для України сьогодні є актуально. Важливо, що суб’єкти такого навчання мають змогу взаємодіяти між собою в зручний для них час, застосовувати одні й ті ж форми і засоби навчальної

діяльності як в аудиторії, так і поза нею, налагоджувати безперервний обмін інформацією за допомогою електронної пошти та месенджерів, ділитися інформацію всередині групи, працювати один з одним. Обидві сторони процесу (педагог і учень) можуть передавати й отримати інформацію на будь-який портативний мобільний пристрій, який підключено до мережі Інтернет, запропонувати чи підшукати необхідний матеріал, опрацювати його, зробити аудіо-/відео-запис тощо.

Під час мобільного навчання, яке є інноваційною методикою, можна використовувати сучасні дидактичні методики, зокрема, застосовувати індивідуальний підхід, розвивати у суб'єктів освіти самостійність і активність, через можливість оперативного доступу до інформації розширювати їхню діяльнісну практичну сферу.

Отже, можна говорити про позитивний вплив мобільних технологій на організацію навчального процесу. Особливо, якщо мова йде про навчання в умовах воєнного стану. Утім, завжди потрібно враховувати те, що використання цієї технології навчання залежить від поширення зв'язку з Інтернетом. Також важливо, щоб застосування інформаційно-комунікаційних технологій було педагогічно виваженим, виправданим, а отже, обґрунтовано теоретично й перевірено експериментальним шляхом.

Література

1. Указ Президента України № 64/2022 «Про введення воєнного стану в Україні» / Указ затверджено Законом України від 24 лютого 2022 року N 2102-IX. URL : https://www.president.gov.ua/documents/642022-41397

2. Вільний тлумачний словник. Новітній онлайновий словник української мови (2013—2018). URL : http://sum.in.ua/f/ghadzhet

УДК 004.6

ПРОТИІМПУЛЬСНИЙ ЗАХИСТ ЯК СКЛАДОВА БЕЗПЕКИ ФУНКЦІОНУВАННЯ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Галас О., Рудик А., Рудик Ю.
Національний університет „Львівська політехніка", Львів
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. Розглядаються пристрої захисту від імпульсної напруги до 1000 В мереж, де використовується чутливе та дороге електрообладнання, яке може бути пошкоджене від короткочасних перенапруг. Наведено підходи до залежності інформаційної безпеки від безпеки апаратної частини, особливо надійності електропостачання у критичних умовах. Їх суть заснована на принципі: безпека хмари – це відповідальність провайдера, безпека мережі – це відповідальність клієнта. Тому питання підвищення безпеки інформаційних мереж потребує різноманітної уваги.

Ключові слова: протиімпульсний захист, вразливість, перенапруга, безпека, якість.

Summary. Protection devices against impulse voltage up to 1000 V are considered for networks where sensitive and expensive electrical equipment is used, which can be damaged by short-term overvoltages. Approaches to the dependence of information security on the security of hardware, especially the reliability of power supply in critical conditions, are presented. Their essence is based on the principle: cloud security is the responsibility of the provider, network security is the responsibility of the client. Therefore, the issue of improving the security of information networks requires various attention.

Key words: anti-pulse protection, vulnerability, overvoltage, safety, quality.

Нині нашою головною метою є вдосконалення діяльності підрозділів ДСНС України, оснащення рятувальників сучасними технічними засобами та налагодження тісної взаємодії з органами місцевої влади у процесі забезпечення цивільного захисту населення. Пристрій захисту від імпульсної напруги призначений для захисту електромережі та електроустаткування від різких змін напруги, які можуть бути викликані, наприклад, ударом блискавки, коротким замиканням або перевантаженням. Такий пристрій підключається до мережі паралельно або послідовно і в пасивному стані ніяк не впливає на роботу іншого обладнання. При різкому зростанні напруги пристрій спрацьовує і вирівнює напругу до безпечного рівня. Промислові підприємства, заводи, лабораторії, медичні установи та інші об'єкти мають складне та дороговартісне електронне обладнання, яке чутливе до перенапруг. У цих випадках пристрої захисту від протиімпульсної напруги можуть бути встановлені на розподільчих щитах, панелях керування, розетках та інших точках живлення, щоб захистити обладнання від комутаційних перенапруг, які можуть бути спричинені перемиканням навантажень, коротким замиканням, процесами корекції коефіцієнта потужності та іншими факторами [1-3].

Один з основних стандартів захисту від імпульсної напруги для пристроїв до 1000 В – це ДСТУ EN 61643-11:2015 Пристрої захисту від перенапруги для низьковольтних систем живлення. Частина 11. Вимоги до продукції та методи випробувань. Цей стандарт визначає загальні та специфічні вимоги до пристроїв захисту від перенапруги для низьковольтних систем живлення (SPD), які поглинають імпульсні струми та напруги. Цей стандарт також описує методи випробувань для перевірки виконання цих вимог [4-5].

За цим стандартом, пристрої захисту поділяються на три класи: I, II та III. Клас I – це прилади захисту від прямих ударів блискавки, які поглинають дуже великі імпульсні струми. Клас II - це прилади захисту від непрямих ударів блискавки, які поглинають помірні імпульсні струми. Клас III – це прилади захисту від залишкових перенапруг, які поглинають невеликі імпульсні струми. За типом захисту, прилади можуть бути L (захист лінії живлення), S (захист сигнальної лінії) або C (захист комбінований) [6]. Для кожного класу приладу захисту передбачені різні методи випробування, які симулюють реальні умови експлуатації. Для мереж ІТ найважливіші ПЗІП третього каскаду класу III, у тестуванні яких використовуються комбіновані імпульси напруги з формою хвилі 1,2/50 мкс та струму з формою хвилі 8/20 мкс, які моделюють залишковий ефект перенапруг [7].

У відповідь на стрімкий розвиток засобів протиімпульсного захисту в результаті загального прогресу сучасних інформаційних та комп'ютерних технологій є необхідність підтримки актуальності систем захисту підприємств від імпульсних перенапруг та безперебійного електроживлення [8].

Загроза безпеки активів об'єкту критичної інфраструктури складається з безлічі пов'язаних і автономних елементів. Розглядаючи загрозу безпеки, як комплекс, виникає ідея пошуку комплексного рішення до потенційної загрози.

Розробляючи комплексну систему протиімпульсного захисту потрібно прослідкувати за вдосконаленням вже існуючих та появу нових організаційних, програмних та технічних способів, які б допомогли в побудові комплексної систем протиімпульсного захисту [9].

Саме правильне проведення процесу розробки комплексної системи протиімпульсного захисту дозволяє оптимізувати як процес реалізації комплексу на практиці, так і гарантувати його максимальну ефективність під час експлуатації.

Підбір компонентів комплексу здійснено враховуючи характеристики об'єкту критичної інфраструктури, елементи якої формували, зокрема, і просторові та бюджетні вимоги [10].

Підійшовши до спроєктованої системи з розширеними параметрами пристрою захисту від імпульсної перенапруги вдалось сформувати картину вразливостей мереж об'єкту критичної інфраструктури під захистом комплексу, та запропонувати способи їх вирішити. З повторенням цієї процедури можна отримати кілька ітерацій параметрів пристрою захисту від імпульсної перенапруги комплексу, з різним рівнем захисту, який буде пропорційним до затрат на його реалізацію та підтримку. Вибір варіанту варто здійснювати оцінюючи ризики.

Література

1. Полотай, О.І. Важливість комплексної системи захисту інформації у забезпеченні інформаційної безпеки ГО “Наукова спільнота”; WSSG w Przeworsku. – Тернопіль, 2022 https://sci.ldubgd.edu.ua/jspui/handle/123456789/11113

2. Ткачук, Р.Л., Сікора, Л.С., Лиса, Н.К., Навитка, М.Л., Сабат, В.І., Федина, Б.І., Тупичак, Л.Л. Інформаційні технології формування стратегій прийняття рішень інтелектуальним агентом в техногенних системах за умов когнітивних збоїв, НУЛП, 2020.

3. Лагун А., Рудик А., Рудик Ю. Аналіз виявлення вразливостей сучасного хостингу при тестуванні на проникнення, Захист інформації в інформаційно-комунікаційних системах, Львів, 2019. С.53-55.

4. Полотай, О.І., Масюк, Н. Профілі можливостей порушників інформаційної безпеки структурних підрозділів безпекових структур Національна Академія Служби Безпеки України, 2021.

5. Ткачук, Р.Л., Боднар, О., Лагун, А. Е. Виявлення небезпечних входжень у комп’ютерну мережу за допомогою систем виявлення вторгнень, ЛДУБЖД, 2021.

6. Захист від імпульсних перенапруг в системах електроживлення: досвід Європи | Компанія WATSON-ENERGO. URL: http://surl.li/nrwju

7. Стандарти BS EN IEC для пристроїв захисту від перенапруги (SPD). Surge Protection Device. URL: https://www.lsp-international.com/uk/free-download-bs-en-iec-standards-for-surge-protective-device-spd/

8. Рудик Ю.І. Захист електроустановок від імпульсних грозових і комутаційних перенапруг. *Пожежна безпека* : зб. наук. пр. Львів, 2009. № 15. С. 89–95

9. ПЗІП SALTEK - захист від імпульсної перенапруги. ТД "Системи Безпеки". URL: https://tdsb.com.ua/saltek-pzip/.

10. Rudyk Yu., Kuts V., Nazarovets O., Zdeb V. Complex tools for surge process analysis and hardware disturbance protection. *Lecture Notes on Data Engineering and Communications Technologies*. 2021. Vol. 69. P. 205–227

УДК: 004.051:004.42

СТАТИЧНИЙ АНАЛІЗ КОДУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Гамрецький Роман, Гнатюк Віктор
Національний авіаційний університет, м. Київ

Анотація. Інформаційно-комунікаційні системи (ІКС) в сучасному світі є визначальним елементом для ефективного функціонування підприємств та організацій. Зростання їхньої складності вимагає створення стабільного та безпечного програмного забезпечення (ПЗ). Статичний аналіз коду виявляє потенційні помилки та забезпечує високу якість ПЗ на ранніх етапах розробки, особливо в критичних ІКС.

Ключові слова: програмне забезпечення, безпека програмного забезпечення, статичний аналіз коду, якість та ефективність коду.

Abstract. Information and communication systems (ICS) in the modern world are a determining element for the effective functioning of enterprises and organizations. Their increasing complexity requires the creation of stable and secure software. Static analysis of the code reveals potential errors and ensures high software quality in the early stages of development, especially in critical ICS.

Keywords: software, software security, static code analysis, code quality and efficiency.

Інформаційно-комунікаційні системи (ІКС) в сучасному світі відіграють ключову роль у забезпеченні ефективного функціонування підприємств та організацій. Зростання їхньої складності та важливість у сучасному суспільстві підкреслює необхідність створення стабільного та безпечного програмного забезпечення (ПЗ). Одним із ефективних інструментів для досягнення цієї мети є статичний аналіз коду (САК).

САК - це процес вивчення програмного коду без його активного виконання. Основна мета полягає в виявленні потенційних помилок, вразливостей та удосконаленні структури коду перед його виконанням [1]. Цей підхід дозволяє розробникам виявляти та виправляти проблеми на ранніх етапах розробки, підвищуючи загальну якість ПЗ.

У сфері ІКС, де надійність та безпека визначають успішність функціонування, САК стає критичним етапом. Застосування САК дозволяє попередити проблеми в ПЗ на ранніх етапах розробки, того його використання рекомендується в критичних системах [1]. Важливо зауважити, що САК може використовуватись не тільки на ранніх етапах життєвого циклу ПЗ, а й в подальшому під час внесення змін чи виправлення помилок.

САК дозволяє [2]:

- виявляти вразливості безпеки: Аналіз коду допомагає визначити потенційні точки доступу для зловмисників та розробників шкідливого ПЗ;
- покращувати ефективність: Ідентифікація та усунення фрагментів коду, які можуть впливати на швидкість та продуктивність системи.
- забезпечувати стабільність: Попередження можливих витоків пам'яті, дефектів та інших аспектів, що можуть призвести до збоїв.

САК – це процес який піддається автоматизації та може бути контрольований за допомогою спеціалізованих інструментів. Це дозволяє автоматично виправляти деякі види помилок. Використання таких інструментів є поширеною практикою під час розробки ПЗ. Серед найбільш поширених інструментів виділяють SonarQube, Better Code Hub, Coverity Scan, FindBugs, PMD та CheckStyle [3]. Також, частина інструментів для статичного аналізу має можливості інтеграції в інтегровані середовища розробки та системи управління версіями.

Застосування статичного аналізу в аспектах безпеки важливо для попередження кібератак та забезпечення високого рівня безпеки ІКС [4]:

- САК дозволяє ідентифікувати потенційні точки вразливості, які можуть бути використані зловмисниками для здійснення атак. Це може включати в себе виявлення неправильного використання критичних функцій, недостатню перевірку введених даних та інші можливі порушення безпеки;
- статичний аналіз може виявити потенційні вразливості, пов'язані з неправильною обробкою SQL-запитів, що дозволяє уникнути атак типу SQL-ін'єкцій та інших векторів атак;
- аналіз коду дозволяє перевірити використання сторонніх бібліотек та компонентів, ідентифікувати їхні версії та перевірити наявність відомих вразливостей. Це сприяє попередженню атак, які можуть бути здійснені через вразливості у використовуваних бібліотеках;
- статичний аналіз може виявити можливі точки витоку конфіденційної інформації. Це включає в себе перевірку, як дані обробляються, передаються та зберігаються, для уникнення ситуацій, коли конфіденційні дані можуть потрапити в ненавмисні руки;
- статичний аналіз дозволяє ідентифікувати потенційні уразливості безпеки, такі як неправильна обробка сесій, відсутність аутентифікації або авторизації, які можуть стати потенційними точками входу для зловмисників;

– статичний аналіз може служити засобом перевірки відповідності програмного коду стандартам безпеки та рекомендаціям, що допомагає забезпечити високий рівень безпеки відповідно до встановлених норм.

Результати статичного аналізу також потребують обробки для ідентифікації та пріоритизації проблем над якими потрібно працювати в першу чергу. Для цього можна застосувати різні експертні системи та штучний інтелект [5].

САК у сфері ІКС визнається обов'язковим інструментом для забезпечення високої якості та безпеки програмних продуктів. Використання статичного аналізу на початкових етапах розробки є стратегічно важливим, оскільки воно сприяє уникненню різноманітних проблем та гарантує ефективне функціонування систем у майбутньому.

Важливість статичного аналізу полягає в тому, що він спрямований на виявлення потенційних помилок, вразливостей та інших аномалій у програмному коді на етапі розробки. Це дозволяє розробникам вчасно виправляти виявлені проблеми, що, в свою чергу, підвищує загальну надійність та якість ПЗ.

На відміну від динамічного аналізу, який виконується під час виконання програми, статичний аналіз не вимагає активного виконання коду. Це дає можливість виявляти потенційні проблеми, які можуть виникнути в реальних умовах експлуатації, вже на етапі розробки.

Використання статичного аналізу на етапах розробки дозволяє зменшити кількість та вартість помилок під час інтеграції та подальшого використання ПЗ. Це ефективний підхід для запобігання виникненню проблем у великих і складних ІКС.

Література

1. Wichmann B. A. et al. Industrial perspective on static analysis //Software Engineering Journal. – 1995. – Т. 10. – №. 2. – С. 69.

2. Bardas A. G. et al. Static code analysis //Journal of Information Systems & Operations Management. – 2010. – Т. 4. – №. 2. – С. 99-107.

3. Lenarduzzi V. et al. A critical comparison on six static analysis tools: Detection, agreement, and precision //Journal of Systems and Software. – 2023. – Т. 198. – С. 111575.

4. Basutakara B. S., Jeyanthi P. N. A review of static code analysis methods for detecting security flaws //J Univ Shanghai Sci Technol. – 2021. – Т. 23. – №. 06. – С. 647-653.

5. Yang X. et al. An Expert System for Learning Software Engineering Knowledge (with Case Studies in Understanding Static Code Warning) //arXiv preprint arXiv:1911.01387. – 2019.

УДК 004.65

ОГЛЯД МЕТОДІВ АНАЛІЗУ СЛАБКОСТРУКТУРОВАНИХ ДАНИХ

Гащук Любомир, Придатко Олександр
Львівський державний університет безпеки життєдіяльності, м. Львів

Проблема обробки слабкоструктурованих даних є актуальною на сьогоднішній день. Проблема полягає в складності обробки масивів цих даних та в їхньому збереженні в базах даних. Слабко структуровані дані це така інформація, яка не має попередньо визначеної моделі, або не має чітко визначеної організації. Часто це можуть бути текстові дані, з яких можна виділити різні параметри або факти які будуть мати дуже нечіткий зв'язок. Така хаотичність в розміщенні даних створює труднощі для їх обробки стандартними програмами аналізу баз даних.

Тим не менше є декілька методів аналізу таких груп даних. Це є інтелектуальний аналіз даних, обробка природної мови і інтелектуальний аналіз тексту. Ці способи дають можливість пошуку зв'язків та закономірностей між даними та можливості їх правильного інтерпретування.

Сучасні методи інтелектуального аналізу даних охоплюють такі задачі, як перетворення, зберігання, аналіз, моделювання та отримання інформації при прийнятті рішень на основі фактичних даних. Data Mining вивчає процес знаходження нових та потенційно корисних знань у базах різноманітних даних. Це комплексний науковий напрям, що знаходиться на перетині таких наук: системи баз даних, статистика, штучний інтелект, дискретна математика, комп'ютерна лінгвістика, теорія графів, теорія алгоритмів тощо. Таким чином можна автоматичним або напівавтоматичним способом аналізувати великі масиви даних та виділяти з них корисні параметри та факти та після цього знайти закономірності та зв'язки між цією інформацією.

Обробка природної мови є напрямком який охоплює роботу зі штучним інтелектом та математичною лінгвістикою. Збоку штучного інтелекту відбувається аналіз мови, а продуктом є генерація розумного тексту. Робота в цьому напрямку буде сприяти зручнішій взаємодії людини та комп'ютера.

Інтелектуальний аналіз тексту є одним з напрямків інтелектуального аналізу даних. Він ставить за мету обробку текстових даних, застосовуючи при цьому методи машинного навчання та обробки природної мови. Аналіз тексту немає великої відмінності від аналізу даних, але різниця є. Різниця проявляється в кінцевих застосовуваних методах та тому що аналізується. Інтелектуальний аналіз даних працює з базами даних, тоді як інтелектуальний аналіз тексту працює з електронними бібліотеками та корпусами текстів.

В науковій статті “Кучук Н. Г. Метод зменшення часу доступу до слабкоструктурованих даних” розглядається метод для оптимізації роботи з слабкоструктурованими даними, використовуючи за основу роботу з множинними запитами до баз даних . В основі цього методу лежить перепланування, яке забезпечує скорочення часу обробки запитів у системи ієрархічних віджетів.

Як висновок, проводиться багато роботи для полегшення обробки слабких даних. Але об’єм даних постійно збільшується, і це сприяє необхідності і надалі досліджувати і створювати нові способи обробки даних.

Література

1. Structure, Models and Meaning: Is «unstructured» data merely unmodeled?, Intelligent Enterprise, March 1, 2005.

2. Silberschatz, Abraham; Sudarshan, S. (2011). *Database system concepts* (вид. 6). New York: McGraw-Hill.

3. Survey of Text Mining I: Clustering, Classification, and Retrieval / Ed. by M. W. Berry. — 2004. — Springer, 2003. — 261 с.

4. Гороховатський, В. О.; Творошенко, І. С. Методи інтелектуального аналізу та оброблення даних: навч. посібник. 2021.

5. Кучук Н. Г. Метод зменшення часу доступу до слабкоструктурованих даних / Н. Г. Кучук, В. Ю. Мерлак, В. В. Скородєлов // Сучасні інформаційні системи = Advanced Information Systems. – 2020. – Т. 4, № 1. – С. 97-102.

УДК 004.5

МЕТОД УДОСКОНАЛЕННЯ РОБОТИ СИСТЕМИ МАСОВОГО ОБСЛУГОВУВАННЯ З ВИКОРИСТАННЯМ ВІРТУАЛЬНОГО АСИСТЕНТА

Гнатюк Віктор, Головань Михайло
Національний авіаційний університет, Київ

Анотація. У роботі проведено аналіз існуючих методів удосконалення роботи системи масового обслуговування, визначено їх переваги та недоліки. З огляду на результати аналізу було розроблено метод удосконалення роботи системи масового обслуговування з використанням віртуального асистента. Розроблене рішення може забезпечувати: покращення взаємодії з користувачами, використання штучного інтелекту для покращення відповідей, ефективне зберігання та аналіз даних.
Ключові слова: СМО, ШІ, GAS.

Abstract. The paper analyzes the existing methods of improving the mass service system, identifies their advantages and disadvantages. Considering the results of the analysis, a method of improving the operation of the mass service system using a virtual assistant was developed. The developed solution can provide: improved interaction with users, use of artificial intelligence to improve answers, efficient storage and analysis of data.
Keywords: MSS, AI, GAS.

Актуальність розробки нових методів удосконалення роботи систем масового обслуговування (СМО) в сучасному світі важлива з кількох ключових причин: поліпшення якості обслуговування, ефективне використання ресурсів, використання сучасних технологій, підвищення конкурентоспроможності бізнесу, відповідь на сучасні виклики та тенденції. Отже, розробка нових методів удосконалення СМО є актуальною науковою задачею, оскільки це може сприяти покращенню якості обслуговування, більш ефективному використанню ресурсів, використанню сучасних технологій та підвищенню конкурентоспроможності бізнесу.

Метою роботи є розробка методу удосконалення роботи систем масового обслуговування, з використанням віртуального асистента на базі штучного інтелекту як ефективного інструменту для автоматизації та поліпшення процесів обслуговування користувачів.

Сучасні методи удосконалення роботи СМО включають в себе велику кількість технологій, моделей та стратегій. Ось низка наукових досліджень сучасних методів: публікація представляє загальну теорію черг та методи оптимізації в СМО [1], публікація присвячена моделюванню та аналізу систем обслуговування, включаючи розподіл завдань між ресурсами [2], стаття присвячена методам оптимізації розподілу ресурсів в хмарних обчисленнях для ефективного обслуговування завдань [3], у статті роз-

глядаються методи оцінки довжини черги та керування дозволом на виклики у мережах зі службами з різними характеристиками [4], у статті пропонуються методи машинного навчання для вибору веб-сервісів з урахуванням якості обслуговування [5]. Ці наукові праці представляють деякі з сучасних методів оптимізації СМО, що використовуються в різних галузях, таких як телекомунікації, хмарні обчислення та веб-сервіси.

З огляду на результати аналізу варто зазначити, що сучасні методи оптимізації СМО мають свої переваги, але також існують певні недоліки. Недоліки сучасних методів оптимізації СМО: складність моделювання, чутливість до параметрів, обмеженість у реальних умовах. Також, варто зазначити переваги СМО з використанням віртуального асистента (ВА) (телеграм бота): автоматизація та ефективність, покращення якості обслуговування, постійна доступність та швидкість відгуку, скорочення витрат, полегшення взаємодії з користувачами. Інтеграція ВА у СМО може допомогти максимально використати переваги автоматизації та поліпшити взаємодію з користувачами. Однак важливо розглядати їх як додатковий інструмент, а не як повноцінну заміну людського фактору та експертності.

Для розробки ВА необхідно обрати інструменти, платформу, до прикладу [6,7], та виконати наступні етапи (рис. 1).

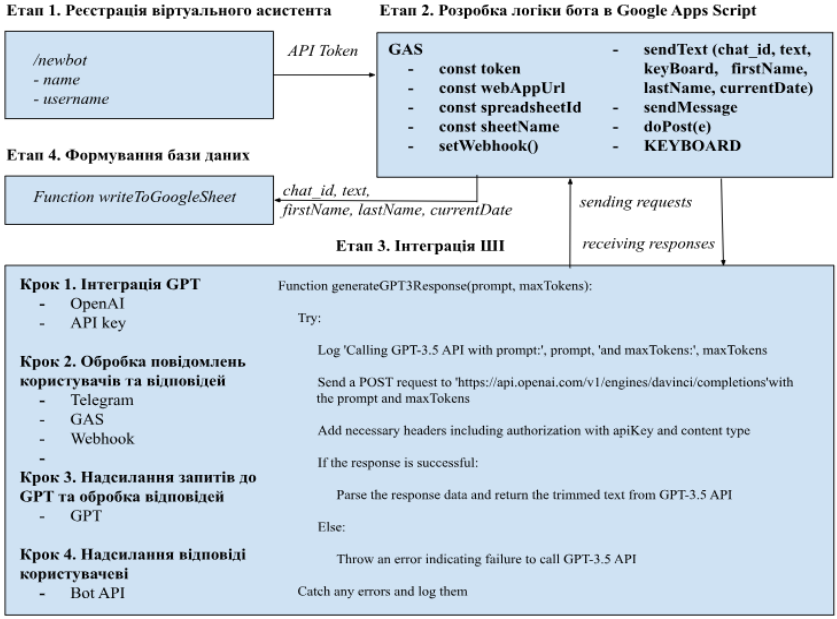


Рисунок 1 – Схема реалізації методу удосконалення роботи СМО з використанням ВА на базі ШІ

Таким чином, розроблене рішення для удосконалення роботи СМО з використанням ВА та інтеграції з GAS, Google Tables та GPT (GPT-3.5). Загальні особливості цього рішення включають наступне: використання Telegram бота (ВА реалізований у вигляді Telegram бота, що забезпечує зручну комунікацію з користувачами через платформу Telegram), взаємодія з користувачами (бот взаємодіє з користувачами за допомогою кнопок та текстових запитів, дозволяючи їм вибирати інформацію, яка їх цікавить), генерація відповідей за допомогою GPT-3.5 (для розширення можливостей ВА використовується GPT-3.5, що дозволяє генерувати більш складні та інформативні відповіді), збереження інформації в Google Tables (інформація про користувачів та їх запити зберігається та управляється в Google Tables, спрощуючи роботу з даними та їх аналіз), використання GAS (використання GAS для програмування логіки бота та забезпечення інтеграції з Google Tables, що дозволяє автоматизувати обробку та збереження даних), оптимізація роботи СМО (ВА та інтеграція з GPT-3.5 спрямовані на оптимізацію обслуговування користувачів, забезпечуючи швидку та інформативну відповідь на їх запити).

Література

1. Kleinrock, L. (1976). Queueing Systems, Volume I - Theory. Wiley. 417 p.

2. Gelenbe, E., & Mitrani, I. (1980). Analysis and Synthesis of Computer Systems. Academic Press. London; New York: Academic Press. 239 p.

3. Ananthanarayanan, G., et al. (2010). CloudScale: Elastic Resource Allocation for Cloud Computing Environments. ACM.

4. Zhang, H., & Hou, J. C. (2005). Queue Length Estimation and Call Admission Control in Differentiated Services Networks. IEEE/ACM Transactions on Networking, 13(2), 400-413.

5. Li, W., & Li, Y. (2009). Learning Automata-based QoS-aware Web Service Selection. IEEE Transactions on Services Computing, 2(1), 48-61.

6. Гнатюк В.О., Бондаренко І.О., Каплун І.С. Використання систем обміну миттєвими повідомленнями для автоматизації надання консультативних послуг. Реєстрація, зберігання і обробка даних. Т 23. № 4. – 2021. – С. 58-67.

7. Гнатюк В.О., Батрак О.Г., Яроцький С.В. Автоматизована система реєстрації місцезнаходження працівника // Проблеми інформатизації та управління: Збірник наукових праць: Випуск 2 (74). К.: НАУ, 2023. С.14-20.

УДК 004.9

ПРОГРАМНА СИСТЕМА «SOS» – ПРІОРІТЕТНИЙ СПОСІБ ЗМЕНШИТИ РИЗИК ВТРАТИ ЖИТТЯ ТА ЗДОРОВ'Я НАСЕЛЕННЯ

Горностай Юрій, Кордунова Юлія
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі проаналізовано та досліджено існуючі методи виклику допомоги в надзвичайних ситуаціях. На основі цього розроблену безпеко-орієнтовану програму "SOS", яка оснащена зручним користувацьким інтерфейсом. Запроваджений підхід дозволить в найкоротший термін викликати екстрену службу допомоги, а також автоматично визначити місцезнаходження потерпілого, що має вирішальне значення коли кожна секунда порятунку людського життя є важливою.

Ключові слова: програма «SOS», Android Studio, безпеко-орієнтований сервіс.

У сучасному світі розробка програмного забезпечення займає ключове місце практично у всіх видах діяльності, галузь безпеки – не виключення. Особливо актуальним в наш час є розробка безпеко-орієнтовних сервісів, які спрямовані на забезпечення порятунку людей та допомоги екстренним службам, при виконанні їх службових обов'язків. Дані сервіси мають важливе значення для інформування та запобігання надзвичайним ситуаціям, ефективності та швидкості реагування на небезпеку, збільшення шансів на порятунок життя людей та мінімізацію можливих втрат. Одним із таких сервісів є розроблена програма "SOS", котра забезпечує негайний виклик екстрених служб та збільшує шанси на забезпечення безпеки людей.

Дана програмна система реалізована на платформі Android Studio та використовує ряд технологій для забезпечення негайного та точного виклику екстрених служб. Однією з ключових особливостей є зручний та інтуїтивний користувацький інтерфейс (Рисунок 1), який використовує функцію натискання кнопки "SOS" (або подвійне натискання кнопки блокування для автоматичного виклику служб та надсилання координат місцезнаходження).

Унікальність програми "SOS" полягає в її здатності об'єднувати в собі простоту використання та високотехнічні можливості, забезпечуючи швидкий та ефективний виклик допомоги в надзвичайних ситуаціях. Такий підхід визначає її перевагу порівняно з іншими методами виклику екстрених служб та робить її незамінною у сфері безпеки та здоров'я людей. Зокрема, дана програма дозволяє уникнути втрат часу на пошук та набір номерів екстрених служб, особливо у стресовій ситуації, та забезпечує автоматичне визначення місцезнаходження надзвичайної події. Такий підхід дозволяє екстреним службам швидше прибути на місце події та збільшує шанси на порятунок.

Рисунок 1 – Інтерфейс програми “SOS”

Розробка програми для виклику екстрених служб передбачає в собі ряд технічних аспектів, що забезпечують швидкість, надійність та безпеку, зокрема:

1. ***Мова програмування:*** використано кросплатформенну мову програмування Java, для роботи в середовищі Android Studio, щоб забезпечити високий рівень сумісності та продуктивності.

2. ***Інтерфейс користувача (UI):*** розроблено інтуїтивний та зручний користувацький інтерфейс, використано бібліотеки та інструменти для реалізації свайпу та обробки жестів (Android ViewFlipper , Android Gesture API , Material Design Components), щоб гарантувати коректну відповідь на дії користувача.

3. **Геолокація та GPS:** використано GPS-модуль Android Location API для автоматичного визначення місцезнаходження користувача.

4. **Система управління дозволами:** забезпечено належні дозволи для доступу до функцій, таких як геолокація та засоби комунікації.

5. **Спрощений виклик екстрених служб:** реалізовано інтерфейс для взаємодії з системою екстрених служб та подальше посередництво в ефективному виклику допомоги.

6. **Заходи безпеки та автентифікації:** впроваджено заходи безпеки, такі як шифрування даних та безпечний обмін інформацією, для захисту конфіденційності користувача.

7. **Оптимізація продуктивності:** враховано оптимізацію для підтримки роботи програми на різних пристроях та версіях операційної системи Android.

8. **Тестування та відлагодження:** включено модульне тестування, тестування в реальних умовах та відлагодження для забезпечення стабільної та надійної роботи.

У результаті була розроблена та досліджена безпеко-орієнтована програма "SOS", як пріоритетний спосіб зменшити ризик втрати життя та здоров'я в надзвичайних ситуаціях. Програма базується на аналізі існуючих методів виклику допомоги та пропонує безпеко-орієнтований сервіс із зручним користувацьким інтерфейсом.

Розробка програми "SOS" є необхідністю у безпековій галузі. Її впровадження у сучасне суспільство може значно підвищити шанси на врятування життя людей та мінімізацію можливих втрат. "SOS" створює новий стандарт ефективної взаємодії між користувачем та екстреними службами, забезпечуючи надійність та швидкість у випадках, де кожна секунда має вирішальне значення.

Література

1. Gosling, J., Joy, B., Steele, G., Bracha G., and Buckley A. (2013) The Java Language Specification, Java Se. *7 Edition*. California, 644

2. Sarkar, A., Goyal, A., Hicks, D., Sarkar, D. and Hazra, S. (2019). Android Application Development: A Brief *Overview of Android Platforms and Evolution of Security Systems*. 73-79. 10.1109/I-SMAC47947.2019.9032440.

3. Kordunova, Y., Prydatko, O., Smotr, O. & Golovatyi, R. (2023). Expert Decision Support System Modeling in Lifecycle Management of Specialized Software. *Lecture Notes in Data Engineering, Computational Intelligence, and Decision Making. ISDMCI 2022. Lecture Notes on Data Engineering and Communications Technologies*, 149, https://doi.org/10.1007/978-3-031-16203-9_22

УДК 004.021

ВИКОРИСТАННЯ СПРЯМОВАНОГО ВИПАДКОВОГО БЛУКАННЯ НА ОСНОВІ ЕНТРОПІЇ ДЛЯ КЛАСИФІКАЦІЇ РАКУ

Гринак Максим
Національний Університет "Львівська політехніка", м. Львів

У даній роботі розглядається використання спрямованого випадкового блукання на основі ентропії для покращення класифікації ракових захворювань. Запропонований метод дозволяє ефективно використовувати інформацію, отриману від випадкового блукання, для вдосконалення точності та надійності класифікаційних моделей.

Ключові слова: спрямоване випадкове блукання, ентропія, класифікація раку, алгоритми, штучний інтелект, directed random walk, entropy, cancer classification, algorithms, artificial intelligence.

Рак є однією з найпоширеніших і найсмертельніших хвороб сучасної медицини. Одним із важливих етапів в діагностиці та лікуванні раку є класифікація пухлин, яка дозволяє визначити їх ступінь злоякісності і вибрати найбільш ефективну стратегію лікування. З метою покращення точності та ефективності класифікації раку, розроблення нових методів є актуальною проблемою. Один зі способів вирішення цієї проблеми полягає у використанні методу спрямованого випадкового блукання на основі ентропії.

Випадковий ліс — це контрольований алгоритм навчання. Він має два варіанти: один використовується для задач класифікації, а інший – для задач регресії. Це один із найбільш гнучких і простих у використанні алгоритмів. Він створює дерева рішень на основі заданих зразків даних, отримує прогноз з кожного дерева та вибирає найкраще рішення шляхом голосування. Це також досить хороший показник важливості функції.

Інтуїцію алгоритму випадкового лісу можна розділити на два етапи. На першому етапі ми випадковим чином вибираємо «k» ознак із загальної кількості m функцій і будуємо випадковий ліс. На другому етапі ми робимо прогнози за допомогою навченого алгоритму випадкового лісу

Алгоритм випадкових лісів можна використовувати для процесу вибору ознак. Цей алгоритм можна використовувати для ранжування важливості змінних у задачі регресії або класифікації.

Ми вимірюємо важливість змінної в наборі даних, пристосувавши до даних алгоритм випадкового лісу. Під час процесу підгонки помилка поза мішком для кожної точки даних записується та усереднюється по лісу.

Ентропія – це міра хаосу системи. Так як вона набагато динамічніша, ніж інші менш мінливі величини, наприклад "частка правильних відповідей" або навіть середньоквадратична помилка, її використання для оптимізації алгоритмів машинного навчання часто призводить до підвищення їх швидкості роботи та продуктивності.

У машинному навчанні її можна зустріти всюди: від побудов дерев рішень до тренувань глибоких нейронних мереж. Ентропія – невід'ємна частина у сфері машинного навчання.

Найчастіше в науці даних ми зустрічаємо середні значення ентропії – між неймовірно високими і ідеально низькими. Висока ентропія відповідає невеликий приріст інформації; низької ентропії, навпаки, великий приріст інформації. Приріст інформації можна визначити як рівень чистоти системи – кількість чистої доступної інформації.

Як можна використовувати ентропію у даному алгоримі:

1. Вибір ознак: Ви можете вибрати певні ознаки або параметри, які визначають патологічні зразки тканини (наприклад, морфологічні ознаки, генетичні дані тощо).
2. Розрахунок ентропії: Для кожного класу (наприклад, "рак" і "здоровий") ви розраховуєте ентропію на основі вибраних ознак. Це допоможе вам виміряти ступінь невизначеності в розподілі цих ознак для кожного класу.
3. Розділення даних: Вибираєте ознаку, за якою можна розділити дані на дві групи, спираючись на розраховану ентропію. Ця ознака має максимально зменшити загальну ентропію системи після розділення, що вказує на те, що ви відокремлюєте різні класи найефективніше.
4. Повторення: Повторюєте процес для нових підгруп даних, досягаючи деревоподібної структури розділень.
5. Класифікація: Коли маєте готове дерево розділень, ви можете використовувати його для класифікації нових зразків на основі їх ознак.

Отже, метод спрямованого випадкового блукання на основі ентропії допоможе побудувати модель класифікації раку, яка використовує ентропію для визначення найкращих ознак і розділення даних на класи. Цей метод може мати потенціал для покращення точності класифікації та діагностики раку

В рамках методологічного дослідження ми спочатку збираємо та підготовку клінічних даних використовуємо з повними формами раку, включаючи клінічні характеристики, генетичні маркери та результат обстеження. Далі, ми шукаємо набір функцій для класифікації, використовуючи націлені випадкові блукання для визначення важливих функцій та їх вагових коефіцієнтів.

На наступному етапі використовуємо різноманітні алгоритми машинного навчання, такі як метод опорних векторів (SVM), випадковий ліс (Random Forest), та нейронні мережі для тренування класифікаційної моделі. Важливо вибрати оптимальні параметри цих алгоритмів для досягнення максимальної ефективності.

Важливою складовою є введення концепції націленого випадкового блукання в алгоритм, що дозволяє ефективно використовувати інформацію про середовище для покращення вибору для навчання та тестування моделі.

Після тренування класифікаційної моделі ми проводимо експерименти для оцінки точності та надійності оптимального методу порівняння з традиційними методами класифікації. Використовуючи метрики, такі як чутливість, специфічність та точність, ми оцінюємо порівняльний аналіз результатів.

У завершеному дослідженні ми проводимо детальний аналіз результатів та шукаємо вплив націленого випадкового блукання на основі ентропії на здатність класифікації моделей, які повністю відповідають та виправляють можливість обмеження методу.

Література

1. Tay, Xin Hui, et al. «An Entropy-Based Directed Random Walk for Cancer Classification Using Gene Expression Data Based on Bi-Random Walk on Two Separated Networks». Genes, p. 574. www.mdpi.com, https://doi.org/10.3390/genes14030574

2. Seah, Choon Sen. An Improved Directed Random Walk Framework for Cancer Classification Using Gene Expression Data. Universiti Tun Hussein Onn Malaysia, eprints.uthm.edu.my, http://eprints.uthm.edu.my/943/

3. Scopus, https://www.scopus.com/standard/marketing.uri

УДК 004

ОСОБЛИВОСТІ СУЧАСНИХ ПРОГРАМНИХ ЕМУЛЯТОРІВ МЕРЕЖЕВОГО ОБЛАДНАННЯ

Губницька Валерія, Ткачук Ростислав, Полотай Орест
Львівський державний університет безпеки життєдіяльності

Описано основні особливості програмних емуляторів мережевого обладнання та їх порівняння

Ключові слова: емулятори мережевого обладнання, комп'ютерні мережі

The main features of software emulators of network equipment and their comparison are described.

Keywords: network equipment emulators, computer networks

Часто при проектуванні локальних обчислювальних мереж використовують аналоги – відомі проектні рішення, що добре зарекомендували себе в роботі, накопичений досвід. Однак, своєрідність та унікальність функцій, що виконуються кожною організацією, їх постійний розвиток, виникнення нових інформаційних технологій обганяють накопичений досвід і тоді локальна обчислювальна мережа, що навіть містить усі сучасні засоби, може працювати з точки зору користувача недостатньо ефективно. При сучасній вартості промислового мережного обладнання помилки, допущені при проектуванні таких мереж, можуть призвести до загроз інформаційної безпеки та фінансових втрат компаній. Саме тому особливий інтерес нині набувають методи, які на основі емулювання мережевого обладнання дозволяють змоделювати майбутню структуру та організацію локальних обчислювальних мереж.

Усі емулятори мережевого устаткування можна розділити на дві основні групи:

1. Апаратно-реалізовані емулятори.
2. Програмно-реалізовані емулятори.

До першої групи відносять, як правило, вузько спеціалізоване устаткування, що дозволяє при підключенні до нього реального телекомунікаційного устаткування імітувати роботу реальної телекомунікаційної мережі, або якоїсь її частини (як правило, каналів зв'язку). Основна мета розробки і застосування апаратних емуляторів – дослідження роботи реального телекомунікаційного устаткування в різних умовах і при різних характеристиках каналів.

До другої групи емуляторів відносять спеціально розроблені програми, що дозволяють імітувати роботу устаткування і каналів зв'язку, а також роботу командних інтерфейсів активного мережевого устаткування. Основна мета використання програмних емуляторів –

застосування в якості науково-дослідної діяльності для постановки наукових експериментів.

Розглянемо основні програмні емулятори мережевого обладнання, порівняльні характеристики яких наведено у таблиці 1.

Найпопулярнішим емулятором мережного обладнання є *Cisco Packet Tracer*, це емулятор, розроблений самою компанією Cisco Systems для навчання фахівців-початківців. Основне призначення емулятора Packet Tracer у створенні віртуальних мереж для проведення практичних робіт для підготовки до сертифікаційних іспитів CCNA (Cisco Certified Network Associate) та CCNA Security (Cisco Certified Network Associate Security). Крім стандартних маршрутизаторів та комутаторів Packet Tracer підтримує емуляцію IP-телефонів, бездротових точок доступу та серверів з набором стандартних служб. У симуляторі реалізовані серії маршрутизаторів Cisco 800, 1800, 1900, 2600, 2800, 2900 і комутаторів Cisco Catalyst 2950, 2960, 3560. Крім того, є сервери DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP і EMAIL, робочі станції, різні модулі до комп'ютерів і маршрутизаторів, смартфони, хаби, а також хмара, що емулює WAN.

GNS3 (Graphical Network Simulator 3) – це незалежний безкоштовний програмний емулятор маршрутизаторів Cisco. GNS3 підтримується в більшості операційних систем Linux, Windows і Mac OS X, при цьому цей програмний емулятор дає можливість емулювати апаратну частину маршрутизаторів Cisco, для цього він завантажує та використовує реальний образ операційної системи Cisco IOS. GNS3 – це графічна оболонка, що поєднує у собі ряд різних програмних засобів емуляції.

EVE-NG (Emulated Virtual Environment - Next Generation) - це емульоване віртуальне середовище наступного покоління, що дозволяє створити повноцінну віртуальну лабораторію з мережевим обладнанням і програмним забезпеченням провідних світових виробників. EVE-NG – це корисний інструмент для сучасного IT фахівця, як для повсякденної роботи, так і для підготовки до сертифікації Cisco рівнів CCNA / CCNP / CCIE, Juniper JNCIA / JNCIP / JNCIE / JNCIS і багатьох інших популярних світових вендорів.

Unified Networking Lab (UNetLab, UNL) – мережевий емулятор, який являє собою розраховану на багато користувачів платформу для моделювання та створення віртуальних мереж, різних лабораторій, що підтримує значний список телекомунікаційного обладнання. UNL дає можливість запуску образів з VIRL (vIOS-L2 та vIOS-L3), образів ASA, Cisco IOL-образів, образів Cisco IPS, образів XRv та CSR1000v, образів dynamips з емулятора GNS, образів Cisco vWLC та vWSA. Крім перерахованих образів підтримується значний список з обладнання інших вендорів: Aruba ClearPass, Alcatel 7750 SR, Arista vEOS, Brocade Virtual ADX, Citrix Netscaler VPX Virtual, Checkpoint Firewall, HP VSR1000, Juniper Olive (porting), Juniper Networks S-Terra Firewall, MS Windows та ін.

Таблиця 1

Порівняльна характеристика аналогів

Характеристика	GNS3	Packet Tracer	EVE-NG	UNetLab
Зручний інтерфейс	+	+	+	+
Можливість використовувати обладнання різних виробників	+		+	+
Запуск справжніх образів обладнання	+		+	+
Потребує багато ресурсів для запуску схеми	+		+	+

Література

1. Полотай О.І., Тлумак О. Вибір обладнання Cisco для розгортання корпоративної VPN-мережі. 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. 64–66.

2. Полотай О.І., Брайко О. Проектування локальної обчислювальної мережі та організація її захисту. Матер. Всеукр. наук.-практ. Інтернет-конф. "Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті : стан, досягнення, перспективи розвитку". Черкаси : ЧНУ ім. Богдана Хмельницького, 2017. С. 58–59.

3. UNetLab: List of supported images [Електронний ресурс] – Режим доступу : http://www.unetlab.com/documentation/supported-images/index.html

4. Eve-ng ltd. Eve-ng Professional Cookbook [Electronic resource]. 2016. [Електронний ресурс]. – Режим доступу з: https://www.eve-ng.net/images/EVE-COOK-BOOK-1.0.pdf.

5. Демянович В. GNS3 – Графічний симулятор мережі, маршрутизаторів Cisco. 2015 [Електронний ресурс]. – Режим доступу з: https://elims.org.ua/blog/gns3-graficheskij-simulyator-seti-marshrutizatorovcisco/

УДК 004.032.26

МЕТОДИ МАШИННОГО НАВЧАННЯ ДЛЯ ПРОГНОЗУВАННЯ НЕЩАСНИХ ВИПАДКІВ

Гудзеляк І., Хлевной О.
Львівський державний університет безпеки життєдіяльності

Машинне навчання може бути використано для автоматизації процесу прогнозування ризикових ситуацій. ML-моделі можуть навчитися виявляти закономірності в даних, які можуть бути використані для прогнозування ризикових ситуацій.

Machine learning can be used to automate the process of predicting risk situations. ML models can learn to identify patterns in data that can be used to predict risk situations.

Ризиковані ситуації є частиною нашого життя. Вони можуть бути пов'язані з безпекою, здоров'ям, фінансами та іншими сферами. Раннє виявлення ризикових ситуацій є важливим завданням, яке може допомогти запобігти нещасним випадкам, хворобам і втратам.

Прогнозування ризикових ситуацій є важливою задачею в багатьох сферах діяльності, таких як безпека, фінанси, медицина та охорона навколишнього середовища. Ця задача полягає в тому, щоб передбачити, коли і де може виникнути ризикова ситуація, щоб можна було вжити заходів для її запобігання або зменшення негативних наслідків.

У традиційному підході до вирішення цієї задачі використовуються статистичні методи, такі як аналіз часу, відсотків та ймовірності. Однак ці методи мають ряд обмежень, таких як необхідність великої кількості даних і неможливість урахування нелінійних залежностей.

Машинне навчання (МН) – це підвид штучного інтелекту, який має справу з розробкою алгоритмів, які можуть навчатися на даних і використовувати ці знання для прогнозування майбутніх результатів. Методи машинного навчання можна використовувати для вирішення широкого спектру задач прогнозування, від прогнозування погоди та цін на акції до прогнозування нещасних випадків, що у свою чергу допомагає попередити їх у майбутньому.

Задача машинного навчання (МН) для прогнозування ризиків виглядає так – нехай є певний відомий набір нещасних випадків та їх детальних описових характеристик. Між випадками та характеристиками є певна прихована залежність. Задача МН – знайти цю приховану залежність для прогнозування нових випадків на основі характеристик нещасних подій.

Основними методами машинного навчання для прогнозування нещасних випадків є регресійні та класифікаційні методи, а також глибоке навчання. Регресійні методи використовуються для прогнозування кількісних показників, таких як кількість нещасних випадків або збитки від нещасних випадків. Класифікаційні методи використовуються для прогнозування категоріальних результатів, таких як тип нещасного випадку або тяж-

кість травм. Глибоке навчання може бути ефективним для прогнозування нещасних випадків, особливо для задач, які вимагають розуміння складних взаємозв'язків між факторами ризику.

Вибір методу залежить від таких факторів, як тип результату, який потрібно прогнозувати, складність та доступність історичних даних за певний період. Також важливим фактором є структурованість описових характеристик нещасних випадків та їх доступність для аналізу. Дані для навчання моделей машинного навчання можуть включати статистичні дані (дату, час, місце, тип нещасного випадку, тяжкість травм) та фактори ризику (характеристики працівника, умови роботи, дані про організацію.

Ефективність моделей машинного навчання для прогнозування нещасних випадків може бути оцінена за такими показниками, як ймовірність того, що модель правильно прогнозуватиме майбутні нещасні випадки або яка ймовірність того, що модель може спрогнозувати нещасні випадки, які відбулися, або яка ймовірність того, що модель правильно прогнозуватиме нещасні випадки, які не відбулися.

Основною перевагою методів машинного навчання для прогнозування нещасних випадків є точність (методи можуть бути дуже точними та ефективними для прогнозування саме нещасних випадків). Також вони можуть бути використані для прогнозування нещасних випадків, які є складними для передбачення та швидкого попередження. Серед недоліків можна виділити наступне: методи можуть бути нестійкими до "шуму в даних", важкі для розуміння та інтерпретації, а часто основною проблемою є висока вартість їх розробки та впровадження.

Методи машинного навчання є доволі ефективним інструментом для прогнозування нещасних випадків, однак для підвищення ефективності моделей машинного навчання важливо використовувати високоякісні(детальні) дані про нещасні випадки та фактори ризику.

Подальші дослідження методів машинного навчання для прогнозування нещасних випадків можуть привести до розробки більш точних та ефективних методів, які можуть бути використані для вирішення цієї серйозної проблеми у різних галузях: безпека праці, безпека дорожнього руху, медицина, промислова безпека.

Література

1. Машинне навчання. Типи навчання.
DOI: https://courses.prometheus.org.ua/courses/IRF/ML101/2016_T3/about

2. . Trevor Hastie, Robert Tibshirani, Jerome Friedman The Elements of Statistical Learning
DOI: https://web.stanford.edu/~hastie/Papers/ESLII.pdf

3. Gong, P., Li, S., & Li, S. (2022). A comprehensive review of machine learning methods for occupational accident prediction. Safety Science, 140, 105349

4. Rai, S., & Agarwal, A. (2022). Machine learning methods for occupational accident prediction: A review. Safety Science, 140, 105344.

УДК 378.14

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ОСВІТНІ ПРОЦЕСИ

Гумен О., Вітченко А.
Український державний університет імені Михайла Драгоманова, Київ

Анотація. Стрімкий технологічний розвиток охоплює всі сфери нашого життя. Вплив інформаційних технологій, які проникають у класичну систему освіти, на освітній процес стає все більш помітним. Визначаємо ключові аспекти цього впливу шляхом вивчення використання комп'ютерів, мобільних пристроїв, Інтернету та соціальних мереж, а також виклики і можливості, які створюються для сучасних закладів освіти.

Ключові слова. Освітній процес, технології навчання, заклад освіти.

Abstract. Rapid technological development covers all areas of our life. The influence of information technologies that penetrate the classical education system on the educational process is becoming more and more noticeable. We identify key aspects of this influence by examining the use of computers, mobile devices, the Internet and social networks, as well as the challenges and opportunities that are created for modern educational institutions.

Keywords. Educational process, learning technologies, educational institution.

Сучасний світ переживає епоху стрімкого технологічного розвитку, і цей розвиток охоплює всі сфери нашого життя. Освітній процес, який десятиліттями був традиційним, трансформується під впливом інноваційних технологій, які проникають у класичну систему освіти і вносять суттєві зміни у підхід до навчання та отримання знань. В умовах глобалізації та зростаючої конкуренції знання та навички стають ключовими ресурсами для успішної кар'єри та особистісного розвитку. Саме тому вивчення впливу інформаційних технологій на навчання та викладання є важливим для розуміння сучасних тенденцій в освіті.

Метою цієї роботи є аналіз та оцінка впливу сучасних технологій на освітні процеси. Визначаються ключові аспекти цього впливу шляхом вивчення використання комп'ютерів, мобільних пристроїв, Інтернету та соціальних мереж в освіті. У роботі також розглядається використання штучного інтелекту та аналітики даних в освіті, а також виклики і можливості, які інформаційні технології створюють для закладів освіти.

Так, використання *комп'ютерів* допомагає створювати інтерактивні навчальні матеріали, спрощує процес збору та аналізу даних і забезпечує доступ до інформації з будь-якої точки світу. До переваг можна також віднести зручність і доступність інформації, економію часу, можливості дистанційного навчання. Останнє особливо важливо, коли стикаєшся з

обмеженнями, спричиненими різними ситуаціями, такими як війна, пандемії чи стихійні лиха. Як недоліки можна виділити відсутність особистого контакту між учасниками освітнього процесу, залежність від технологій, відсутність саморегуляції.

Використання *мобільних пристроїв*, таких як смартфони та планшети, у навчанні стає дедалі популярнішим завдяки їхній мобільності та доступу до різноманітних освітніх програм і ресурсів. Переваги: різноманітні навчальні програми та додатки, розроблені для полегшення навчання, доступ до різних джерел інформації. Недоліки: відволікання, адже соціальні мережі, ігри та інші розважальні програми можуть легко відволікти увагу від навчання; втома від екрану, коли занадто багато часу, проведеного перед екранами мобільних пристроїв, може призвести до втоми і погіршення зору.

Інтернет та соціальні мережі є важливим аспектом сучасної освіти. Перевагами їх використання є можливість широкого обміну інформацією, що сприяє співпраці та командному навчанню, а також розширює можливості для дискусій та обміну ідеями; доступ до якісної освіти з віддалених місць через онлайн-курси; доступність та різноплановість ресурсів. У той же час існують значні ризики інформаційного перевантаження і впливу фейків.

Перевагами використання *штучного інтелекту та аналізу даних* в освіті є персоналізоване навчання, можливість прогнозування академічної успішності студентів, ефективність навчання, адже викладачі можуть отримувати дані про те, як студенти взаємодіють з навчальними матеріалами, коригувати методи викладання та надавати додаткову підтримку студентам, які її потребують. Незважаючи на ці переваги, використання штучного інтелекту та аналізу даних в освіті також пов’язане з певними проблемами, а саме: необхідність забезпечення конфіденційності даних, небезпека надмірного покладання на технології. Підсумовуючи, можна сказати, що використання штучного інтелекту та аналітики даних в освіті може значно покращити навчання і сприяти підвищенню успішності студентів. Однак важливо ретельно продумати захист інформації і плани резервного копіювання, щоб забезпечити надійність освітнього процесу.

Сучасні технології, безсумнівно, відіграють ключову роль у трансформації освітнього процесу та створенні нових можливостей для навчання і розвитку навичок, компетенцій та вмінь. Переваги використання технологій в освіті очевидні. Вони надають доступ до величезних обсягів інформації, сприяють інтерактивному та персоналізованому навчанню, полегшують спостереження та аналіз успішності учнів і надають можливості для вдосконалення освітнього процесу. Крім того, це відкриває шлях для розвитку онлайн-освіти і

забезпечує доступ до якісної освіти для студентів по всьому світу. При цьому важливо пам'ятати про численні виклики, пов'язані з використанням технологій в освіті. Конфіденційність даних учасників освітнього процесу є серйозним питанням, і важливо забезпечити їх захист. Покладання на технології також є ризиком, оскільки технологічні проблеми можуть призвести до зриву освітнього процесу.

Інформаційні технології надають навчальним закладам широкий спектр можливостей для покращення навчання та доступу до освіти. Однак для досягнення найкращих результатів їх використання потребує ретельного планування, фінансування розвитку та підготовки викладачів. Заклади освіти повинні бути готовими до змін. Фінансові обмеження та необхідність навчати викладачів користуватися новими технологіями вимагають інвестицій і зусиль. Однак ці виклики можна подолати завдяки ретельному плануванню та достатнім ресурсам.

Збалансоване поєднання традиційних освітніх методів і сучасних інформаційних технологій є запорукою успіху. Освіта повинна вдосконалюватися, але не втрачати зв'язку з глибинними освітніми цінностями. Розвиток освіти у світлі сучасних технологій має сприяти створенню інтелектуально розвиненого, творчого та інноваційного суспільства. Таким чином, вплив технологій на освітній процес є складною і багатогранною темою, яка потребує постійного дослідження та адаптації до нових реалій. Зберігаючи баланс між традиціями та інноваціями, освіта може стати потужним інструментом суспільного розвитку та досягнення індивідуальних і колективних цілей.

Література:

1. Anderson, T., & Dron, J. (2011). Three generations of distance education pedagogy. The International Review of Research in Open and Distributed Learning, 12(3), 80-97.

2. Bates, A. W., & Sangrà, A. (2011). Managing technology in higher education: Strategies for transforming teaching and learning. John Wiley & Sons.

3. Selwyn, N. (2017). Education and technology: Key issues and debates. Bloomsbury Publishing.

4. Ertmer, P. A., & Ottenbreit-Leftwich, A. T. (2010). Teacher technology change: How knowledge, confidence, beliefs, and culture intersect. Journal of Research on Technology in Education, 42(3), 255-284.

УДК 374.71:004

"КАМЕНІ СПОТИКАННЯ" ПРИ ВИКОРИСТАННІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ

Гуменюк Микола, Каращук Віталій
Вище професійне училище Львівського державного університету безпеки життєдіяльності (м. Вінниця)

Анотація: Тези доповіді носять інформаційний характер і містять факти та аргументи щодо проблем, які виникають при застосуванні інформаційних технологій в освіті. Виділено чотири групи проблем (каменів спотикання), які сьогодні є актуальними та беззаперечними і потребують негайного вирішення задля гармонійного розвитку суспільства шляхом використання інформаційних технологій при формуванні загальних та спеціальних компетентностей.

Ключові слова: кіберсоціум, медіаграмотність, *кіберхарассмент, дезінформація,* штучний інтелект.

Abstract: The abstracts of the report are informative in nature and contain facts and arguments regarding the problems that arise in the application of information technologies in education. Four groups of problems (stumbling blocks) are highlighted, which today are relevant and indisputable and require an immediate solution for the harmonious development of society through the use of information technologies in the formation of general and special competencies.

Keywords: cyber society, media literacy, cyberharassment, disinformation, artificial intelligence.

Інноваційні технології в освіті майже всі інформаційні, всі розвиваються та апробовуються із шаленими темпами. Звісно, що сьогоднішнього педагога ними не здивуєш, адже він немає вибору при використанні їх у професійній діяльності. Виникає питання "Чому так?". Пояснення в тому, що події, які складаються (пандемії та епідемії, військова агресія, інтенсивна диджиталізація) максимально зобов'язують педагога опановувати інформаційні технології аби "йти в ногу з часом". Тим паче сучасна молодь настільки підкована у їх використанні (кіберсоціальна), що без них заняття їм нудні, пасивні та малоефективні. Але, чи означає це, що учасники освітнього процесу знають та розуміють усі плюси та мінуси використання інформаційних технологій? Чи достатньо вони проінформовані щодо захисту персональних даних? Чи достатньо вони мають розвинені навички медіагігієни та медіаграмотності? Чи вміють вони фільтрувати інформацію, яка різнокольоровими барвами сприймається візуально й майже не піддається сумніву? Подібних питань десятки і всі вони сьогодні перебувають у статусі "відкриті" та "актуальні".

Відкритість та актуальність таких питань зумовила появу безлічі онлайн курсів, семінарів, вебінарів та інших заходів, які спрямовані на

вирішення і поліпшення якості інформаційної освіти серед учасників освітнього процесу [1]. Розуміємо, якщо не реагувати на рівень подібних питань і їх не помічати, то виникає високий ризик мінливої поведінки людини до дезінформації, схильності до маніпуляцій, схильності до проявів інтернет-жорстокості тощо. Звідси виникає перший "камінь спотикання", який по ідеї майже не очевидний. Щодо фактів, які свідчать про його місце є розміщені результати дослідження рівня інформаційної гігієни серед користувачів соціальної мережі Facebook в одному із номерів газети "Українська правда" [2]. У підсумку — 73 % користувачів не мають навичків дотримання інформаційної гігієни та інформаційної медіаграмотності. Отож можемо сміливо припустити, що результати опитування щодо використання інформаційних технологій в освіті будуть майже ідентичними. Із ряду дослідницьких робіт маємо цифру в 50 %. Додатковими аргументами на попередні думки є випадки кібербулінгу та кіберхарассменту[1] серед учасників освітнього процесу.

Другим "каменем спотикання" є захист персональних даних таких як: адреса електронної скриньки, номер мобільного телефону, інформація про особу, адреса проживання тощо. Багато із користувачів інтернет-програмами та додатками мало задумується про їх значення. Тому, сьогодні широко розповсюджені різного роду інтернет-шахрайства, мобінг та фішинг. Зловмисники різними способами намагаються отримати цінну інформацію для шахрайських дій із банківськими рахунками, особистим листуванням, тощо. Навіть звичайна реєстрація на цільовому сайті може загнати користувача у тенети аферистів. Погодьтеся, що реєстрація сьогодні здебільшого обов'язкова для користування будь-яким інтернет-продуктом і, навіть якщо вона безпечна, гарантії того, що не буде розсилок спаму ніхто не дає. Адже спам-розсилки це майже гарантія шахрайства [3, с. 278-283].

Зміст третього "каменя спотикання" полягає у тому, що використання освітніх інформаційних технологій в деякому аспекті призводить до втрати навичків критичного і математичного мислення, комунікативних компетентностей та граматики. Існує думка, що педагогам краще використовувати гаджети як зброю задля освіти. Але це далеко хибна думка. В результатах дослідження PISA[2], що опубліковані в мережі Інтернет, в приблизно 25% здобувачів освіти відсутній базовий рівень природничо-математичної грамотності, а в 33% - базовий математичний [4]. То чи такі результати не спричинені інтенсивним використанням гаджетів та освітніх додатків? Слід задуматися і пам'ятати, що застосування інформаційних технологій має бути доречним, доцільним та порційним.

---

[1] англ. harassment — пригнічення

[2] Programme for International Student Assessment — міжнародна Програма з оцінювання освітніх досягнень

Поява штучного інтелекту (ШІ) призвела до розвитку четвертого "каменя спотикання". Програми із елементами штучного інтелекту сьогодні пишуть твори, наукові роботи, статті, картини, програми тощо. З однієї сторони важко оцінити таку роботу на наявність плагіату, з іншої — відсоток особистої діяльності здобувача освіти. Не важко поміркувати і прийти до висновку, що штучний інтелект створює в освітньому процесі більше проблем чим користі.

Отже, інформаційні технології в освіті мають як свої переваги, так і недоліки. Залежно від обраної сторони можна наводити безліч фактів та аргументів, проте слід чітко розуміти з якою метою вони використовуються. Усі зусилля мають бути направлені на формування навичків роботи із інформацією, здатності протидіяти фейкам, дезінформації тощо. Освітяни мають використовувати освітні інформаційні технології не задля "хайпу", а задля максимального формування у підопічних загальних та спеціальних компетентностей. Слід пам'ятати педагогічну мораль, яка говорить: "Застосування інформаційних технологій в освіті значно індивідуалізує освітній процес, збільшує швидкість і якість засвоєння навчального матеріалу, дозволяє істотно посилити практичну спрямованість, розвинути творчі здібності здобувачів освіти, а також навчити їх самостійно мислити і активно працювати з навчальним матеріалом".

Література

1. Портал цифрового перетворення України E-UKRAINE. Режим доступу: https://eukraine.org.ua/ua/news/top-12-osvitnih-majdanchikiv-z-bezkoshtovnimi-onlajn-kursami. (Дата звернення 19.10.2023).

2. Інтернет-видання газети "Українська правда". Режим доступу: https://www.pravda.com.ua/articles/2021/04/6/7289090. (Дата звернення 25.10.2023).

3. Сабадаш В.П. Інтернет-шахрайство реалії сучасності і криміналістичні аспекти протидії. // Наукові записки Таврійського національного університету імені В.І. Вернадського.// Серія: Юридичні науки. Том 26 (65) №1.

4. Офіційний веб-сайт Програми з оцінювання освітніх досягнень PISA. Режим доступу: https://www.oecd.org/pisa.

УДК 37.018.3:004.7

ІНФОРМАТИЗАЦІЯ ОСВІТИ

Дам-Васильєва Чанг Анжеліка, Сорокін Степан
Харківський національний університет радіоелектроніки, м. Харків

Rapid informatization changes everyday life and education. Information technologies are vital for training specialists in automated work environments. This work examines the essence, strategies, trends and educational consequences of informatization of education.

Keywords: information, information technology, education, automation, trends.

Стрімка інформатизація змінює повсякденне життя та освіту. Інформаційні технології життєво необхідні для підготовки спеціалістів в автоматизованих робочих середовищах. У цій роботі досліджується суть, стратегії, тенденції та освітні наслідки інформатизації освіти.

Ключові слова: інформатизація, інформаційні технології, освіта, автоматизація, тенденції.

В галузі освіти інформатизація відкрила можливість доступу до глобальних інформаційних ресурсів, зробила освіту менш залежною від фізичного місцеположення учасників, сприяла процесу глобалізації, покращила якість і зміст навчального процесу та підвищила ефективність освітніх матеріалів [1].

Навчальні інформаційні технології визнаються як сучасний підхід до навчання, який активно використовує комп'ютери та програмне забезпечення для досягнення своїх цілей [2]. Міжнародні експерти та вчені також підтверджують важливість та необхідність інтеграції інформаційних технологій у сферу освіти. Тим самим інтерактивність та використання мультимедійних засобів допомагають кращому усвідомленню та засвоєнню інформації.

Головна мета використання технологій в навчанні полягає в тому, щоб учні відчували себе комфортно у сучасному інформаційному суспільстві. Інформаційні технології сприяють розвитку інформаційної грамотності та навичок роботи з комп'ютерами. Але використання комп'ютерів вимагає розуміння їхньої роботи та функцій.

Також використання комп'ютерів у навчанні може вирішити одну з ключових проблем - низьку успішність [3]. Впровадження комп'ютерних технологій в навчання може стимулювати пам'ять, розвивати спостережливість та аналітичні здібності, концентрувати увагу учнів і навчати їх критично оцінювати подану інформацію. Комп'ютери розширюють можливості представлення навчального матеріалу. Різні

ситуації та середовища можуть бути відтворені за допомогою кольорів, графіки, звуку та відео-техніки. А це може збільшити інтерес студентів до навчання [4].

Однак існують значні труднощі на цьому шляху, переважно пов'язані з недостатнім або нульовим фінансуванням розвитку освітніх закладів. Крім того, для успішного впровадження цих технологій необхідні висококваліфіковані вчителі та постійний професійний розвиток [4].

Ми перебуваємо у 21 столітті, яке можна назвати інформаційною ерою. Ефективне використання інформації як стратегічного ресурсу для розвитку цивілізації має величезне значення, і від цього залежить не лише процвітання і стабільність наших суспільств, але й наша здатність подолати глобальні проблеми.

Тому процес інформатизації нашого життя, пов'язаний із поширенням комп'ютерної техніки в освіті, обов'язково сприятиме створенню нових технологічних інструментів для розв'язання потенційних проблем [4].

Література

1. Allreferat. (2023, 7 листопада). Інформаційні технології в освіті. https://allreferat.com.ua/uk/pedagogika_metoduka_vukladanny/kontrolnaya/5888

2. nformacijninavcanna. (2023, 6 листопада). Інформаційні технології навчання. https://sites.google.com/site/informacijninavcanna/

3. Darynalennon. (2023, 6 листопада). ІНДЗ з дисципліни «Сучасні інформаційно-комунікаційні технології навчання» Макаренко Дарина https://sites.google.com/site/darynalennon/

4. Освіта.ua. (2023, 7 листопада). Сучасні інформаційні технології у школах. https://osvita.ua/school/method/34855/

УДК 378.147.091.31

ДОСВІД ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРОЦЕСІ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ВИКЛАДАЧІВ НАВЧАЛЬНО-МЕТОДИЧНИХ ЦЕНТРІВ ЦИВІЛЬНОГО ЗАХИСТУ

Демків Анна, Власенко Євген, Скоробагатько Тарас, Тищенко Василь
Інститут державного управління та наукових досліджень з цивільного захисту

Анотація: стаття присвячена питанням професійного розвитку викладачів навчально-методичних центрів цивільного захисту (НМЦ ЦЗ) та удосконалення підвищення кваліфікації шляхом використання інформаційних технологій.

Ключові слова: інформаційні технології, викладач, підвищення кваліфікації.

Abstract: is devoted to the issues of professional development of teachers of educational and methodical centers of civil defense (EMC CD) and improvement of professional development through the use of information technologies.

Keywords: information technology, lecturer, advanced training.

Інформаційні технології в освіті – це комплекс навчальних і навчально-методичних матеріалів, технічних та інструментальних засобів техніки навчального призначення, а також система наукових знань про роль і місце технологій в навчальному процесі, про форми і методи їх застосування для вдосконалення праці викладачів.

За півтора роки війни в Україні склалися умови, коли модернізація педагогічних технологій з урахуванням дистанційних форм навчання стала гострою потребою в контексті забезпечення якісних освітніх послуг. Онлайн-технології отримали достатньо широкий розвиток. Технології навчання ґрунтуються на певному змісті і мають відповідати вимогам його представлення (подання). На рис. 1 наведено класифікацію інформаційних технологій дистанційного навчання (ДН) запропонованою науковцем Н. Думанським.

Слід зазначити, що сьогодні в розпорядженні науково-педагогічних працівників (НПП) системи післядипломної освіти в сфері цивільного захисту та викладачів НМЦ ЦЗ, є багато безкоштовних і зручних онлайн-сервісів, які можна використовувати на різних етапах ДН. Наприклад, для комунікації між суб'єктами освітнього процесу використовують: соціальні мережі, зокрема Facebook; блоги, чати викладачів, НПП – де ведуться записи, публікуються завдання та терміни їх виконання, посилання на навчально-методичні матеріали, здійснюється обмін «постами»; залишаються коментарі і додаткові посилання для підвищення інтерактивності; електронне листування, які містять навчально-методичні матеріали (презентації, відео, книги, методичні рекомендації тощо); відеоуроки – використання YouTube-каналу (відеозаписи уроків у відповідності з навчальною програмою).

Рисунок 1 – Класифікація інформаційних технологій дистанційного навчання (за Н. Думанським).

Використання хмарних сервісів також є достатньо поширеною практикою роботи із слухачами курсів підвищення кваліфікації. Це: створення тестів із використанням Google Forms; набір сервісів, які уможливлюють організацію освітнього процесу онлайн: Google Classroom, Microsoft Teams, Cisco Webex, Zoom, Class Dojo, Classtime, Viber та інші. Їх функціональна гнучкість дає змогу викладачу зустрічатися зі слухачами, перевіряти рівень засвоєння знань, вести дискусії, здійснювати експертну оцінку, працювати в групах тощо (наприклад, BigBlueButon). Для проведення віртуальних конференцій, семінарів, вебінарів тощо викладачами широко використовуються онлайн-платформи: Zoom, Skype, GoogleMeet.

Упродовж багатьох років для підвищення кваліфікації викладачів НМЦ ЦЗ в ІДУНДЦЗ застосовується онлайн-платформа MOODLE, яка забезпечує організацію ДН з метою підтримки балансу теорії та практики з різноманітними видами завдань. За останні п'ять років система ДН на платформі MOODLE в ІДУНДЦЗ продемонструвала значний потенціал в організації підвищення кваліфікації різних фахівців з питань цивільного захисту, також використовувалась для організації навчання в системі післядипломної освіти у формі змішаного навчання. Вченими доведено, що впровадження системи ДН з використанням LMS MOODLE сприяє розвитку освітнього менеджменту, «переводить діяльність усіх суб'єктів навчання в більш продуктивний режим, оскільки чітко її організує в просторі і часі (Петренко, 2018), надає можливості переглядати презентації з окремих навчальних тем (дисциплін), та узагальнено основні переваги застосування LMS MOODLE для організації ДН – «гнучкість системи, зручність, модульність, інтерактивність, різні форми контролю знань, журнал успішності, планування подій тощо» (Осадча, Осадчий, Спірін, Круглик, 2021).

В освітній практиці педагогічних працівників НМЦ ЦЗ пріоритетного значення набувають технології навчання, побудовані на взаємодії суб'єктів навчання. Це інтерактивне навчання, яке здійснюється як співнавчання, взаємонавчання, під час якого слухачі й викладачі є рівноправними, рівнозначними суб'єктами.

За результатами вивчення наукової педагогічної, психологічної, методичної літератури нами з'ясовано, що розроблення технологій професійного розвитку викладачів НМЦ ЦЗ є одним із аспектів сучасної післядипломної освіти, спрямований на підвищення якості навчання та розвитку професійно-педагогічної компетентності викладачів. Застосування таких технологій сприяє мотивації викладачів у процесі підвищення кваліфікації і в міжкурсовий період їх професійному розвитку. Йдеться про такі технології: веб-семінари та відеокурси (організація онлайн-семінарів та відеокурсів за допомогою спеціальної платформи); електронні платформи навчання; взаємне спостереження та колегіальні заняття (організація системи спільного спостереження дає можливість викладачам переглядати уроки одного, обговорювати сильні та слабкі сторони і надавати зворотний зв'язок); менторство та коучинг (більш досвідчені викладачі надають підтримку менш досвідченим колегам, допомагають вирішувати професійні проблеми та розвивати їхні навички); дослідницькі проекти; самоосвіта (підтримка вчителів у самостійному отриманні нових знань та вмінь за допомогою доступних онлайн-ресурсів, книг, журналів тощо); система оцінювання професійного зростання (відстежує професійний розвиток викладача, його досягнення та залучення до різноманітних професійних заходів); регулярний обмін досвідом (організація регулярних зустрічей, семінарів, конференцій, вчителі можуть обмінюватися досвідом, навчальними матеріалами та успішними практиками).

Література

1. Думанський, Н. (2008). *Класи сучасних технологій дистанційної освіти*. Національний університет "Львівська політехніка", кафедра інформаційних систем та мереж. Львів. URL: http://vlp.com.ua/files/12.pdf

2. Демків, А. (2023). Педагогічні умови професійного розвитку викладачів навчально-методичних центрів цивільного захисту в процесі підвищення кваліфікації. *Освіта дорослих: теорія, досвід, перспективи, 1 (23), 60-69.* DOI: 10.35387/od.1(23).2023.60-69

3. Петренко, Л. (2018). Організаційні методи дистанційного навчання в закладах професійної (професійно-технічної) освіти. *Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми.* (50), 151-156. URL: http://nbuv.gov.ua/UJRN/mitimpt_2018_50_30

4. Осадча, К., Осадчий, В., Спірін, О., Круглик, В. (2021). Реалізація індивідуалізації та персоналізації навчання засобами MOODLE. *Молодь і ринок.* 1 (187), 38–43. URL:http://mir.dspu.edu.ua/article/view/228274/227419

УДК 004.8:656.078.5

ВИКОРИСТАННЯ ОБЧИСЛЮВАЛЬНОГО ІНТЕЛЕКТУ ДЛЯ УПРАВЛІННЯ ПРОЄКТАМИ РОЗВИТКУ ТРАНСПОРТНОЇ ІНФРАСТРУКТУРИ

Демчина Василь
Львівський державний університет безпеки життєдіяльності

Проаналізовано сучасні інформаційні технології та можливість їх використання для управління проектами розвитку транспортної інфраструктури. Означено моделі та алгоритми обчислювального інтелекту, які використовуються для управління проектами розвитку транспортної інфраструктури. Обгрунтовано доцільність використання машинного навчання, комп'ютерного зору, розпізнавання мови, інтелектуальних систем підтримки прийняття рішень та нечіткої логіки для управління проектами розвитку транспортної інфраструктури.

Ключові слова: обчислювальний інтелект, управління, проекти, розвиток, транспортна інфраструктура

Modern information technologies and the possibility of their use for managing transport infrastructure development projects are analyzed. Computational intelligence models and algorithms used to manage transport infrastructure development projects are defined. The expediency of using machine learning, computer vision, speech recognition, intelligent decision support systems, and fuzzy logic for managing transport infrastructure development projects is substantiated.

Keywords: computational intelligence, management, projects, development, transport infrastructure

Сучасні інформаційні технології залишаються невід'ємною частиною проектного управління. У останні роки спостерігається збільшення кількості наукових праць, у яких автори пропонують використовувати обчислювальний інтелект для вирішення задач у різних сферах діяльності, у тому числі і у проектному менеджменті. Обчислювальний інтелект – це галузь інформатики, яка зосереджена на розробці алгоритмів і програм, здатних виконувати завдання, які зазвичай вимагають людського інтелекту. Обчислювальний інтелект включає в себе широкий спектр напрямів, який включає машинне навчання, комп'ютерний зір, розпізнавання мови, прийняття рішень і нечітку логіку.

Нами у вигляді таблиці 1 представлено різні напрямки обчислювального інтелекту, а також моделі та алгоритми, які використовуються для управління проектами розвитку транспортної інфраструктури (табл. 1).

Таблиця 1 – Моделі та алгоритми обчислювального інтелекту, які використовуються для управління проектами розвитку транспортної інфраструктури

Напрям обчислювального інтелекту	Моделі та алгоритми для управління проектами розвитку транспортної інфраструктури
Машинне навчання	Прогнозування обсягів транспортних потоків на основі врахування історичних даних із сформованих великих баз даних. Виявлення раціональних сценаріїв реалізації проектів розвитку транспортної інфраструктури із мінімальними витратами ресурсів та обмеженими бюджетами.
Комп'ютерний зір	Відстеження та аналіз великих обсягів даних з використанням відеоспостереження для контролю за проектним середовищем та реалізацією проектів розвитку транспортної інфраструктури.
Розпізнавання мови	Автоматичний аналіз та відсіювання інформації з різних джерел комунікації між стейкхолдерами проектів розвитку транспортної інфраструктури.
Нечітка логіка	Розробка моделей, методів та алгоритмів для виконання процесів управління проектами розвитку транспортної інфраструктури із врахування невизначеності та ризиків проектного середовища.
Інтелектуальні систем підтримки прийняття рішень	Розробка моделі та алгоритмів із використанням технологій обчислювального інтелекту, які лежать в основі інтелектуальних систем підтримки прийняття рішень, що забезпечують точний та швидкий аналізу даних проектного середовища та реалізації проектів, а також отримання рекомендацій для прийняття оперативних та стратегічних рішень під час виконання процесів управління проектами розвитку транспортної інфраструктури.

Представлена таблиця 1 демонструє, як окремі напрямки обчислювального інтелекту можна використати для виконання різних процесів управління проектами розвитку транспортної інфраструктури. Однією з ключових переваг технологій обчислювального інтелекту є те, що є можливість комбінування інструментарію із різних його напрямків для створення комплексних інтелектуальних інформаційних систем. Саме це забезпечує обґрунтування та оптимізацію різних груп управлінських процесів впродовж етапів життєвого циклу проектів розвитку транспортної інфраструктури та вдосконалюють рішення.

Машинне навчання може допомогти покращити точність прогнозування транспортних потоків на основі історичних даних, що забезпечує якісний інструментарій для планування та зниження обсягів використання ресурсів під час реалізації проектів розвитку транспортної інфраструктури. Також цей напрям забезпечує визначення раціональних сценаріїв реалізації проектів.

Відстеження та аналіз великих обсягів даних на основі технологій комп'ютерного зору використовують для ефективного відстеження реалізації робіт у проектах розвитку транспортної інфраструктури та для контролю за ними.

Автоматичний аналіз та відсіювання непотрібної інформації: із використанням технологій розпізнавання мови може полегшити процес комунікацій між стейкхолдерами, дозволяючи ефективніше взаємодіяти та уникати можливих конфліктів.

Розробка моделей для управління ризиками із використанням нечіткої логіки забезпечує врахування невизначеності та ризиків у проектному середовищі, що лежить в основі підвищення точності управлінських рішень стосовно проектів розвитку транспортної інфраструктури та забезпечує обґрунтування та використання адаптивних сценаріїв під час управління зазначеними проектами.

Інтелектуальні системи підтримки рішень, які засновані на технологіях обчислювального інтелекту, дають змогу отримати точний та швидкий аналіз даних, а також обґрунтувати якісні рекомендації для прийняття оперативних та стратегічних рішень.

На підставі представленого матеріалу можна зробити висновок, що використання обчислювального інтелекту для управління проектами розвитку транспортної інфраструктури є дуже перспективним напрямком. Використання таких технологій, як машинне навчання, комп'ютерний зір, розпізнавання мови, інтелектуальні системи підтримки прийняття рішень та нечітка логіка, може значно підвищити ефективність управління проектами, зменшити ризики та витрати, а також покращити комунікацію між стейкхолдерами. Для подальших досліджень необхідно розробляти методи та моделі для створення комплексних інтелектуальних систем, які враховують різні аспекти управління проектами розвитку транспортної інфраструктури.

Література

1. Tryhuba A., Zachko O., Grabovets V., Berladyn O., Pavlova I., Rudynets M. Examining the effect of production conditions at territorial logistic systems of milk harvesting on the parameters of a fleet of specialized road tanks. Eastern-European Journal of Enterprise Technologies. 2018. 5(3). P. 59-70.

2. Tryhuba, A., Kondysiuk, I., Tryhuba, I., Boiarchuk, O., Tatomyr, A., Intellectual information system for formation of portfolio projects of motor transport enterprises. CEUR Workshop Proceedings, 2022, 3109, pp. 44–52.

3. Ratushny R., Tryhuba A., Bashynsky O., Ptashnyk V. Development and usage of a computer model of evaluating the scenarios of projects for the creation of fire fighting systems of rural communities. XI-th International Scientific and Practical Conference on Electronics (ELIT-2019). 2019. P. 34-39.

4. Tryhuba A., Bashynsky O. Coordination of dairy workshops projects on the community territory and their project environment. 14th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), 2019. 3. P. 51-54.

5. Придатко О., Лясковська С., Мартин Є., Хлевной О. Моделювання багатопараметричних систем. Львів: ЛДУ БЖД, 2021. 245 с.

УДК:004

ІНТЕРАКТИВНІ МЕТОДИ НАВЧАННЯ ІЗ ЗАЛУЧЕННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Дендаренко Владислав
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля НУЦЗ України, м. Черкаси

Сучасне навчання без залучення інформаційних технологій не може бути повноцінним. Нижче розглянуто можливості використання інформаційних технологій в навчанні. Інтерактивні online-дошки та можливості, які вони надають, методи додаткового спілкування викладача та студента, а також можливості, які надають планшетні комп'ютери в навчанні.

Modern education cannot be complete without the involvement of information technologies. The possibilities of using information technologies in education are considered below. Interactive online whiteboards and the possibilities they provide, methods of additional communication between the teacher and the student, as well as the possibilities provided by tablet computers in education.

Інтерактивні методи навчання являють собою підхід до освіти, в якому студенти активно взаємодіють з навчальним матеріалом, викладачами та один з одним. Ці методи спрямовані на створення змістовного навчального середовища та заохочення студентів до самостійного мислення та вивчення.

Основними характеристиками інтерактивних методів навчання можуть бути такі методи, як групова робота, використання технологій, а також ділові ігри та симуляції. Використання групової роботи дозволяє студентам обмінюватися ідеями, вирішувати завдання та вчитися один у одного. Цей метод сприяє розвитку комунікаційних навичок та співпраці. Застосування сучасних інформаційних технологій, таких як інтерактивні дошки, віртуальна реальність чи мобільні додатки, створює інтерактивність в навчальному процесі та залучає студентів до активного вивчення матеріалу. Ділові ігри та симуляції дозволяють студентам відтворювати реальні ситуації та вирішувати проблеми, що сприяє розвитку критичного мислення та практичних навичок.

Більшою мірою на цей час розвиваються та застосовуються саме методи засновані на інформаційних технологіях, саме вони розвивають не тільки критичне мислення та навички в тій чи іншій сфері, а й системне мислення завдяки своїй послідовності та багатогранності використання. Інформаційні технології в навчанні відіграють важливу роль, змінюючи традиційний підхід до освіти та розширюючи можливості студентів та викладачів.

Заміна традиційних паперових підручників електронними дозволяє студентам з легкістю отримувати доступ до актуальної інформації завдяки швидкому і простому пошуку, а також використовувати мультимедійні елементи для кращого розуміння матеріалу. Використання відеоконференцій, онлайн-лекцій та платформ зробили дистанційне і гібридне навчання реальним і в тих напрямках де непотрібно спеціалізоване обладнання такий підхід може прийти на заміну заочній формі, яка давно втратила свою ефективність і по суті, просто перевтілюється в дистанційну.

Інтерактивні дошки, такі як Miro, Padlet, Conceptboard дозволяють залучати студентів до активного навчання і надають велику кількість можливостей серед яких:

- інтерактивність, що надає можливості викладачам створювати інтерактивні заняття, включаючи анімації, графіки та інші візуальні елементи;
- спільна робота над проектами та під час вирішення важливих завдань в режимі реального часу покращую колективне навчання та розвиває навички роботи в команді і є корисним як для виконавців так і для майбутніх керівників;
- запис і відтворення занять можливе за допомогою функції вставки відеофрагментів, що надає більш широке розуміння викладеного матеріалу;
- віртуальні екскурсії та експерименти притаманні як онлайн-дошкам, так и окремим онлайн-лабораторям;
- легкість доступу з будь-якого пристрою, що має Інтернет-підключення дає смогу навчатись і навчати скрізь і в будь-який час і є незамінною перевагою в сучасному насиченому житті.

Навчання в сучасних умовах вже неможливе старими методами і однією з нових течій є використання планшетних комп'ютерів які можуть замінити практично все окрім натурних зразків. Технології збору, зберігання і передачі інформації надають планшету шанс замінити підручники, які раніше потрібно було носити на кожне заняття, а використання зручного і швидкого пошуку прискорить пошук того, чи іншого місця в літературному джерелі, яке може бути звичайним документом у форматі PDF. Технології підтримки стілуса роблять із планшета портативний конспект по всім предметам, що необхідні студенту. З цією метою можуть використовуватись такі застосунки як Notion, goodnotes та concept. З усіма своїми можливостями навіть безкоштовні версії дають достатньо можливостей для ведення рукописних конспектів з можливостями вставки зображень, таблиць, текстових фрагментів та фото з необхідними матеріалами.

Не менш важливими в навчанні є і хмарні технології, які використовуються в усіх вищеперелічених продуктах і методах, але для звуження поняття поставимо наголос конкретно на хмарних просторах для накопичення, використання та передавання інформації таких як box, dropbox, google drive, mega та інші. Використання даних елементів дистанційної роботи і навчання назавжди звільняє нас від постійного місця роботи, або навчання. За допомогою них студенти можуть починати працювати над проектом в одному місці, а продовжувати або закінчувати в іншому, налагодивши при цьому сумісну роботу з друзями і навіть надавши доступ викладачу для перевірки роботи на будь-якому етапі.

Всі ці можливості дистанційної роботи і навчання на даному етапі розвитку освіти є незамінним і обов'язковим елементом. Без миттєвого сповіщення про проведення додаткових консультацій викладачем одразу з наданням посилання та цю консультацію в WhatsApp або Chat сучасна освіта неможлива. Поштові клієнти із можливістю фільтрації листів на різні мітки не втрачає актуальності і сьогодні і продовжує бути незамінним методом спілкування викладача із студентом разом із месенджерами та застосунками для відеоконференцій, такими як Zoom та Meet.

Інтерактивні методи навчання відкривають нові можливості для підвищення якості освіти, заохочуючи активну участь студентів та розвиваючи необхідні навички для успішної адаптації до сучасного суспільства.

Література

1. Дендаренко В.Ю. Використання сервісу Evernote для організації робочого простору: збірник матеріалів всеукраїнської науково-методичної конференції "Сучасні методи та форми організації освітнього процесу у закладах вищої освіти". 21 черв. 2022 р. / М-во освіти і науки України, ДЗ Південноукраїнський національний педагогічний університет імені К.Д. Ушинського. О.: ПУНПУ ім. К.Д. Ушинського, 2022. – 96 с.

УДК 681.6.012

ВПЛИВ ВИБОРУ МАТЕРІАЛУ ТА СПОСОБУ ДРУКУ НА ЯКІСТЬ 3D ДРУКУ

Дерпак Орест
Львівський національний університет природокористування

Мета даного дослідження полягає в систематичному аналізі впливу різних методів 3D друку та вибору матеріалів на якість виготовлених об'єктів. Досліджуються ключові методи: FDM, SLA, DMT. Вивчаються основні показники якості, такі як роздільна здатність, міцність та гладкість поверхні.
Ключові слова: 3D друк, адитивні технології, FDM, SLA, DMT.

The purpose of this study is to systematically analyze the influence of various 3D printing methods and the choice of materials on the quality of manufactured objects. Key methods are studied: FDM, SLA, DMT. Basic quality indicators such as resolution, strength and surface smoothness are studied.
Key words: 3D printing, additive technologies, FDM, SLA, DMT.

У світі, де технології швидко розвиваються, 3D друк визначає нові стандарти виробництва та дизайну. Важливим аспектом цього процесу є вибір методів друку та матеріалів, оскільки вони безпосередньо впливають на якість та характеристики виготовлених об'єктів. Надійність та точність надрукованих виробів має велике значення і в воєнних реаліях України, оскільки деякі частини для дронів не виготовляються фабрично, і єдиним швидким виходом є 3D друк.

FDM є однією з найпопулярніших технологій 3D друку, використовуючи різні полімери для створення об'єктів. PLA, екологічно чистий і біорозкладний матеріал, знаходить застосування в прототипуванні та декоративних виробах. ABS, з високою міцністю, ідеальний для деталей, що вимагають стійкості [1]. PETG комбінує в собі міцність ABS і зручність PLA. TPU використовується для гнучких деталей, додавши аспект гнучкості до можливостей друку.

Технологія SLA використовує різні смоли, що визначають властивості друку. [4] Стандартні смоли підходять для точних прототипів, гумові смоли використовуються для гнучких виробів, а термостійкі смоли забезпечують вироби, що витримують високі температури [2]. SLA забезпечує високу роздільну здатність і можливість створювати складні форми, зробивши його відмінним вибором для прецизійного друку.

Також можна відмітити технологію [3]. DLP яка теж має досить високу роздільну здатність та швидкість експозиції, дозволяючи експонувати весь шар смоли одразу. Її універсальність дозволяє працювати з різними матеріалами та створювати об'єкти з різними властивостями. Однак існують недоліки,

такі як обмежений робочий об'єм, висока вартість пристроїв, обмежений вибір матеріалів та чутливість виробів до впливу світла та температур.

Упродовж останніх років в світі спостерігається активна імплементація 3D друку в різні сфери життя. Адитивні технології успішно вийшли за рамки етапу зародження і знаходять застосування не лише у промисловому секторі, а й у різних інших галузях. Найнадійнішим та найточнішим є метод друку SLA, який використовує різні смоли, що визначають властивості друку. Стандартні смоли підходять для точних прототипів, гумові смоли використовуються для гнучких виробів, а термостійкі смоли забезпечують вироби, що витримують високі температури, технологія забезпечує високу роздільну здатність і можливість створювати складні форми.

Література

1. High Definition 3D Printing – Comparing SLA and FDM Printing Technologies. Tyler Finnes 2015. 18c

2. Degnan, Michael. 3D Printing Techniques and Processes. Сполучені Штати Америки, Cavendish Square Publishing LLC, 2017. 128c.

3. Fink, J. K. 3D Industrial Printing with Polymers. Сполучені Штати Америки: Wiley. 2018. 342c.

4. Horvath, J., Cameron, R. . Mastering 3D Printing: A Guide to Modeling, Printing, and Prototyping. Німеччина: Apress. 2020. 347c.

УДК 004.032.26

ЗАДАЧА ПЕРЕДБАЧЕННЯ В КОНТЕКСТІ DATA SCIENCE

Дзедзінський Я.О.
Приватний заклад вищої освіти ІТ СТЕП Університет, Україна, Львів

Анотація. Задача передбачення в Data Science відіграє центральну роль у сучасному аналізі даних, використовуючи статистичні та машинні алгоритми для виведення прогнозів з існуючих даних. Ця публікація зосереджується на ключових методах, викликах та практичному застосуванні цих технік.

Ключові слова: Data Science, машинне навчання, статистичний аналіз, прогнозування, глибинне навчання, аналіз даних.

Вступ. Задача передбачення (prediction task) в машинному навчанні та аналітиці даних відноситься до процесу використання моделі, натренованої на історичних даних, для прогнозування майбутніх або невідомих значень цільової змінної. Ця цільова змінна може бути як дискретною (класифікація), так і безперервною (регресія).

Сенс “задачі передбачення" в контексті Data Science відноситься до процесу аналізу інформації з метою передбачення майбутніх подій або результатів. Це ключовий елемент у багатьох областях, таких як фінанси, маркетинг, медицина та інженерія. Суть цієї задачі полягає у використанні історичних даних для навчання моделей, які можуть виявляти закономірності та тенденції, за допомогою яких можна робити обґрунтовані прогнози про майбутнє.

У Data Science передбачення часто здійснюється за допомогою методів машинного навчання та статистичного аналізу. Ці методи дозволяють комп'ютерам "навчатися" з даних і робити прогнози або приймати рішення без явного програмування для кожного конкретного випадку. Важливими аспектами задачі передбачення є вибір правильного алгоритму, точне збирання та обробка даних, а також оцінка точності та надійності прогнозів.

Мета дослідження. У цьому дослідженні прагнеться розглянути та аналізувати різні підходи та методики у задачі передбачення в контексті Data Science, з акцентом на їхню ефективність, точність та практичне застосування у різних сферах.

Ключові аспекти:

- Аналіз підходів: Розгляд різних методів машинного навчання, статистичного аналізу та глибинного навчання, зіставлення їх переваг і недоліків.
- Оцінка точності та надійності: Вивчення впливу якості даних, вибору моделі та обробки даних на точність прогнозування.

- Застосування у різних сферах: Аналіз практичного використання цих методів у важливих областях, таких як фінанси, охорона здоров'я, маркетинг тощо.
- Виклики та майбутні тенденції: Визначення основних викликів у сфері передбачення та прогнозування майбутніх напрямків розвитку в цій області.

Очікуваний результат. Дослідження має на меті не тільки надати глибоке розуміння сучасних тенденцій і практик у передбаченні в Data Science, але й сприяти розробці більш ефективних і точних методів аналізу даних, які можуть бути застосовані для розв'язання складних задач в різноманітних галузях.

Задачі передбачення в різних галузях застосовуються в бізнесі, фінансах, медицині, екології, інженерії, транспорті та багатьох інших сферах, де аналітичні моделі можуть бути корисними для прогнозування майбутніх подій на основі вже наявних даних.

Висновок. Задача передбачення в Data Science є динамічною і багатогранною, вимагаючи постійного розвитку та адаптації. Розуміння та ефективне використання цих технік має вирішальне значення для розвитку багатьох індустрій та секторів.

Література

1. Іванова, А. (2020). "Моделі та методи машинного навчання в аналізі даних." Київ: Наукова думка.

2. Brown, L. & Smith, J. (2021). "Predictive Analytics in Data Science: Trends, Techniques, and Applications." Oxford: Oxford University Press.

3. Кузнєцов, М. (2019). "Статистичний аналіз та його роль у Big Data." Львів: Львівська політехніка.

УДК [004.42+005.6]:378.1

АЛГОРИТМ РОБОТИ ІНФОРМАЦІЙНО-ДОВІДКОВОЇ СИСТЕМИ "UNIBELL"

Дзень Віталій, Бик Еміль, Борзов Юрій
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. У роботі висвітлені особливості алгоритму роботи інформаційно-довідкової системи швидкого доступу до бази даних навчального розкладу. Подано модель клієнтської та серверної частин системи. Описано особливості взаємодії клієнтської та серверної частин системи.

Ключові слова. База даних, розклад, мобільний додаток, алгоритм застосунку

Abstract. The paper describes the algorithm of the information and reference system of access to the curriculum database. The model of client and server part of the system is given. Features of interaction of client and server part of system are described.

Keywords. Database, schedule, mobile application, application algorithm

Модернізація освітнього середовища в сучасних умовах потребує постійного удосконалення існуючих та розроблення нових сервісів, які націлені на забезпечення якості здобуття освіти. Не виключенням стало створення інформаційно-довідкової системи «UniBell» на базі Львівського державного університету безпеки життєдіяльності. Інформаційно-довідкова система орієнтована на швидкий доступ до бази навчального розкладу за допомогою мобільних технологій.

Інформаційно-довідкова система побудована за клієнт-серверною архітектурою. Користувацький інтерфейс реалізовано у вигляді мобільного додатку під операційну систему Android. Серверна частина призначена для завантаження, зберігання, пошуку та обробки даних, а також підтримки працездатності системи.

На рисунку 1 представлено концептуальну модель даної системи у вигляді алгоритму роботи клієнтської частини застосунку.

Алгоритм роботи цієї частини застосунку відповідає за реакцію дій користувача та її взаємодію із сервером. За умови авторизації користувача його дані заносяться до реєстру та зберігаються там до моменту нової авторизації на мобільному пристрої. Збереження даних про авторизованого користувача потрібне для формування та надсилання миттєвих автоматичних запитів через «Головне вікно» при вході у додаток залежно від обраного фільтру (запит на сьогодні, на завтра, на визначену дату). Для формування спеціалізованих (індивідуальних) запитів за певними критеріями пошуку (викладач, група, аудиторія) інформація про авторизованого користувача не

приймається до уваги, а пошукове розпорядження формується за допомогою передбачених фільтрів у «Вікні пошуку». Ще один варіант пошукових розпоряджень може готуватись на стороні клієнта за допомогою вбудованої опції QR-сканування, в результаті чого формується запит на отримання інформації про заняття у визначеній аудиторії в режимі реального часу.

Основне призначення роботи серверної частини в автоматичному режимі – це опрацювання запитів, що надходять з клієнтської частини та зворотне надсилання результатів їх обробки через блок взаємодії з клієнтом.

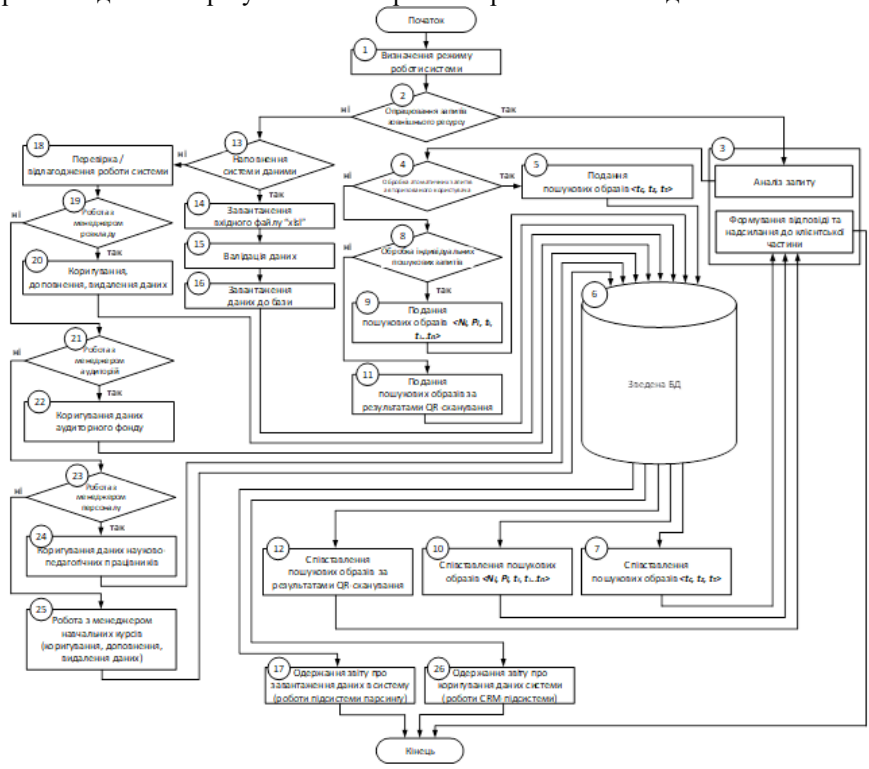


Рисунок 1 – Алгоритм роботи клієнтської частини системи «UniBell»

Залежно від того, який запит було сформовано на клієнтській стороні, його опрацювання передається на відповідний блок обробки (автоматичних запитів, стандартних запитів або індивідуальних пошукових запитів). Після порівняння пошукових образів у базі даних отримана інформація у структурованому вигляді надсилається до клієнтської частини та відображається на мобільному пристрої.

Висновки. Шляхом розроблення специфікації та побудови алгоритму із використанням програмних технологій .Net, Java і мови структурованих запитів SQL розроблено функціонуючу інформаційно-довідкову систему для організації віддаленого доступу до бази даних навчального розкладу із використанням мобільних технологій, що відповідає концепції проєкту Smart-університет.

Література

1. Burak, N., & Rak, Yu. (2014). Модель проектно-інформаційного середовища покращення підготовки рятувальника в ментальному просторі ІТ-технологій. Вісник Львівського державного університету безпеки життєдіяльності. 10, 24–32.

2. Malets, I., Popovych, V., Prydatko, O., Dominik, A. (2018). Interactive Computer Simulators in Rescuer Training and Research of their Optimal Use Indicator. 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), 2, 558-562. https://doi.org/10.1109/DSMP.2018.8478486

3. Prydatko, O., Prydatko, V., Borzov, Yu., & Dzen V. (2018). Integration of the new method of mobile education in educational projects of programmer training. Bulletin of Lviv State University of Life Safety, 18, 71-80. https://doi.org/0.32447/20784643.18.2018.07

УДК [004.942+005.5]: 614.84

КОНЦЕПЦІЯ МОДЕЛІ ОБРОБКИ ОПЕРАТИВНИХ ДАНИХ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Дідушок С.О., Борзов Ю.О., Придатко О.В.
Львівський державний університет безпеки життєдіяльності

Анотація: в роботі представлена концептуальна модель організації оперативного обміну інформацією між підрозділами Державної служби України з надзвичайних ситуацій. Модель включає базові принципи організації процесу обміну оперативними даними на регіональному рівні зважаючи на нову організаційно-штатну структуру територіальних підрозділів.
Ключові слова: оперативні дані, обмін інформацією, організаційно-штатна структура.

Abstract: the work presents a conceptual model of organizing the operational exchange of information between units of the State Emergency Service of Ukraine. The model includes the basic principles of organizing the process of operational data exchange at the regional level, taking into account the new organizational and staffing structure of territorial divisions.
Keywords: operational data, information exchange, organizational and staff structure.

Зважаючи на укрупнення адміністративно-територіальних районів в межах області реформаційних процесів зазнала і організаційно-штатна структура територіальних управлінь ДСНС України в областях. В межах новостворених центрів адміністративно-територіальних районів області функціонують новостворені районні управління. В склад районних управлінь входять Державні пожежно-рятувальні загони, які об'єднують під собою Державні пожежно-рятувальні частини та інші рятувальні формування, а також здійснюють координування роботи місцевих пожежних команд. В оперативному відношенні Державні пожежно-рятувальні загони в режимі добового чергування підпорядковуються оперативно-координаційному центру ГУ ДСНС України в області. Координацію дій підрозділів під час реагування на надзвичайні події, обмін інформацією, відомче та міжвідомче інформування забезпечує оперативно-диспетчерська служба оперативно-координаційного центру ГУ ДСНС України в області.

За існуючої моделі прийому і опрацювання екстрених викликів за межами адміністративного центру області, вони надходять на пункти зв'язку Державних пожежно-рятувальних частин, що розміщені в адміністративних центрах районів (районних центрах). Далі диспетчер пункту зв'язку організовує надсилання підрозділів до місця виклику, здійснює доповідь про подію до ОДС ОКЦ та організовує маршрутизацію і обмін інформацією між ОДС ОКЦ та підрозділами, що перебувають на місці ліквідації надзвичайної події.

Проте, у зв'язку із укрупнення адміністративно-територіальних районів та включенням районних центрів за старим районуванням до складу новоутворених районів, модель прийому і опрацювання викликів, а також реагування на надзвичайні події, може не задовольняти реальні умови оперативного функціонування підрозділів ДСНС України. Уся інформація щодо штатного розпису, наявності особового складу, ланок ГДЗС, техніки на чергуванні у підпорядкованих підрозділах новостворених районів на рівні Державного пожежно-рятувального загону (за нової моделі територіального підпорядкування). А отже першочергові рішення, щодо надсилання підрозділів на місце події та координування їх роботи, можуть приймати диспетчера пунктів зв'язку ДПРЗ зважаючи на наявну інформацію щодо сил і засобів та місць перебування підрозділів. Відповідно, прийом та опрацювання повідомлень про надзвичайні події рекомендовано здійснювати через пункти зв'язку центральних підрозділів Державних пожежно-рятувальних загонів.

Подальша маршрутизація інформації з місця ліквідації до пункту зв'язку ДПРЗ може здійснюватися через диспетчерів пунктів зв'язку ДПРЧ, за умови відсутності технічної можливості передачі інформації каналами прямого зв'язку.

Щодо прийому та опрацювання повідомлень про надзвичайні події в межах обласного центру та його конгломерату, то ці повноваження рекомендовано залишити за оперативно-диспетчерською службою оперативно-координаційного центру при ГУ ДСНС України в області (залишається класична модель прийому та опрацювання повідомлень про надзвичайні події, а також координування роботою підрозділів). Описану модель представлено на рисунку 1.

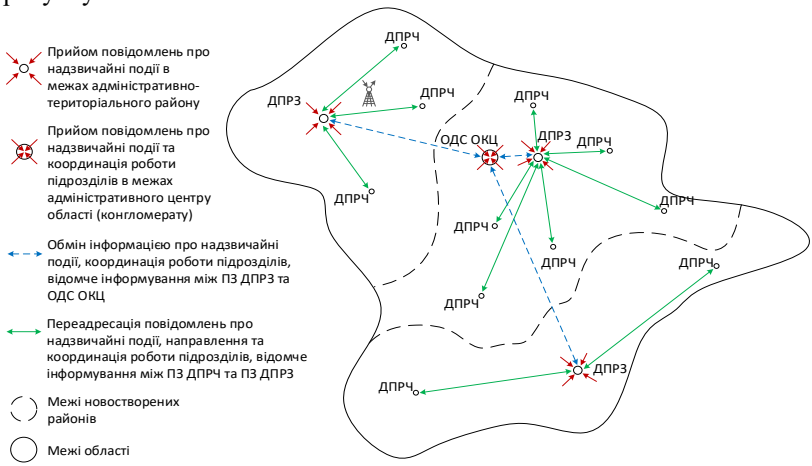


Рисунок 1 – Умовна візуалізація моделі прийому і опрацювання екстрених викликів та реагування на надзвичайні події (регіональний рівень)

Описану модель, представлено у вигляді структурно-логічної схеми (рисунок 2).

Рисунок 2 – Модель прийому і опрацювання викликів

Висновки: За результатами аналізу існуючих технологій організації зв'язку та особливостей регіонального адміністративно-територіального поділу, обґрунтовано оптимальні способи маршрутизації інформації з місця ліквідації надзвичайної події до пункту зв'язку ДПРЗ (ОДС ОКЦ), а також розроблено концептуальну модель прийому і опрацювання екстрених викликів, що дозволило обґрунтувати рекомендації для налагодження стабільного процесу обміну оперативними даними між підрозділами ДСНС на регіональному рівні за умов запровадження нової організаційно-штатної моделі управління.

Література:

1. Informational System of Project Management in the Areas of Regional Security Systems' Development / O. Prydatko, O. Smotr, Yu. Borzov, I. Solotvinskyi, O. Didyk // 2018 IEEE Second Conference on Data Stream Mining & Processing. – 2018. – №2. – С. 187-192.

2. Shcherbachenko O. Organizational and technological backgrounds of project configuration management for firefighting / O. Shcherbachenko // TEKA an international quarterly journal on motorization, vehicle operation, energy efficiency and mechanical engineering. – 2017. – №3(17). – С. 49-53.

3. Придатко О. В. Модель портфельного управління проектами розвитку регіональних систем безпеки життєдіяльності / О. В. Придатко, І. В. Солотвінський, І. Я. Кокотко, М. Б. Івановський // Управління розвитком складних систем : Зб. наук. праць. К. : КНУБА, 2018. – №36. – С.42-51.

УДК 004.9

ІНФОРМАЦІЙНА СИСТЕМА ОРГАНІЗАЦІЙНОЇ ПІДТРИМКИ РОБОТИ ЛАНКИ ГАЗОДИМОЗАХИСНОЇ СЛУЖБИ

Дмитрук Богдан
Львівський державний університет безпеки життєдіяльності

У роботі описано концепцію роботи телеграм бота для збору даних та розв'язок часу роботи ланки ГДЗС. Бот призначений для облегшення, та пришвидшення розрахунків на посту безпеки.

Ключові слова: програмне забезпечення, телеграм бот, база даних, пост безпеки.

The paper describes the concept of the telegram bot for data collection and the solution of the time of operation of the GDZS link. The bot is designed to facilitate and speed up calculations at the security post.

Keywords: software, telegram bot, database, security post.

При прибутті на пожежу постовий на посту безпеки зобов'язаний розраховувати:

- найбільшу витрату тисків під час прямування до осередку пожежі,
- розрахувати тиск при якому ланка має покинути осередок пожежі,
- час роботи на місці пожежі,
- очікуваний час повернення ланки з НДС.

Ці розрахунки можна автоматизувати, зменшивши час обрахунку, та вірогідність помилки (людський фактор).

Чат бот призначений для облегшення розв'язання задач. Постовий вносить дані в бота, а він їх зберігає в базі даних. Дані необхідні для обчислення:

- показання манометрів;
- часу входу в середовище непридатне для дихання;
- кількість чоловік, тип апаратів;
- початковий тиск апаратів;
- тиск апарату при прибутті;
- умови гасіння.

Після коректного вводу всіх даних в БД, бот бере дані з бази і підставляє в формули. Обчислює і виводить дані:

- тиск виходу ланки;
- час роботи на місці пожежі;
- очікуваний час повернення ланки.

На фото зображено прийняття, обробка даних та відправлення повідомлення в чат бота.

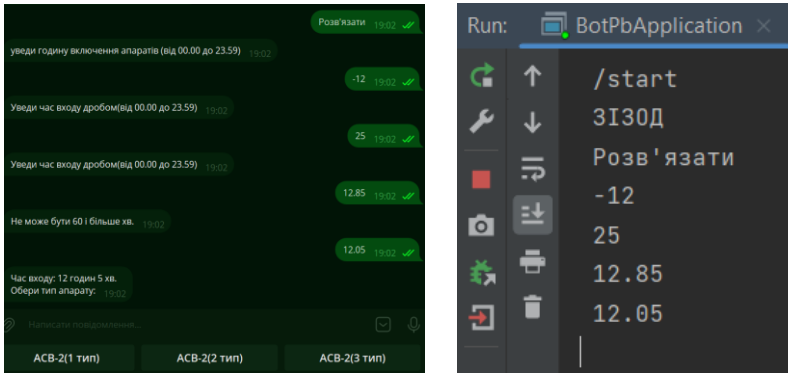


Рисунок 1 – Візуалізація роботи чат-боту

Після реалізації буде проведено тестування та усунення всіх недоліків, які будуть виявлені під час роботи.

Останньою частиною стане розробка програми для розумних годинників та телефонів, котрі будуть сигналізувати ланку ГДЗС про те, що час покинути місце гасіння пожежі. Також розробка off-line калькулятора розрахунку часу роботи ланки ГДЗС.

Література

1. Придатко О. В., Бурак Н. Є., Дзень В. Є., Кунинець М. С. Запровадження інформаційно-довідкової системи "UNIBELL" у освітнє середовище вищого навчального закладу. Ukrainian Journal of Information Technology. 2020, Вип.2, №1. С. 57-65. https://doi.org/10.23939/ujit2020.02.057

УДК 519.2

МЕТОДИ І ЗАСОБИ ВІЗУАЛІЗАЦІЇ ДЛЯ СТАТИСТИЧНОЇ ОБРОБКИ ДАНИХ

Думас Мартин, Карабин Оксана
Львівський державний університет безпеки життєдіяльності, м. Львів

Анотація: розглянуто найбільш доступні програмні засоби, які дозволяють швидко і легко справитись з візуалізацією статистичної інформації, зокрема можливості додатку Data Analysis пакету EXCEL.
Ключові слова: візуалізація даних, описові статистики, пакет аналізу.

Abstract: the most available software tools that allow you to quickly and easily cope with the visualization of statistical information, in particular the capabilities of the Data Analysis application of the EXCEL package, are considered.
Keywords: data visualization, descriptive statistics, analysis package.

Статистичний аналіз займає вагоме місце для моделювання і прогнозування процесів і явищ, зокрема він є ключовим компонентом для будь якого проекту машинного навчання. За допомогою статистичного аналізу можна встановити закономірності, кореляції та зв'язки у великих наборах даних. Перед початком процесу аналізу необхідним є процес візуалізації даних, який може мати різні форми залежно від поставленої проблеми.

Так, для перевірки статистичних гіпотез про закон розподілу випадкових величин потрібно побудувати гістограму, щоб мати візуальну уяву про можливе припущення щодо того, який закон розподілу найбільш точно відповідає статистичній сукупності. Для здійснення кореляційного аналізу та побудови регресійної моделі потрібно мати візуальну картину форми залежності: лінійна залежність, чи нелінійна. Таку візуалізацію можна здійснити за допомогою діаграми розсіювання. Для багатомірного регресійного аналізу такою візуалізацією можуть бути кореляційні матриці.

Розглянемо найбільш доступні програмні засоби, які дозволяють швидко і легко справитись з візуалізацією статистичної інформації.

Для статистичної обробки найбільш доступний і зручний в користуванні є пакет EXCEL. Зокрема в цьому пакеті є можливість підключення пакету аналізу (Data Analysis) , в який входить багато інструментів, серед яких є інструмент побудови гістограми (Histogram) одночасно з побудовою інтервального статистичного розподілу. На рис. 1. наведено приклад гістограми і інтервального розподілу, побудованих за допомогою підключеного пакету аналізу.

Bin	Frequency
292	4
302	10
312	14
322	20
332	22
342	15
352	3
362	6
372	5
382	1
More	0

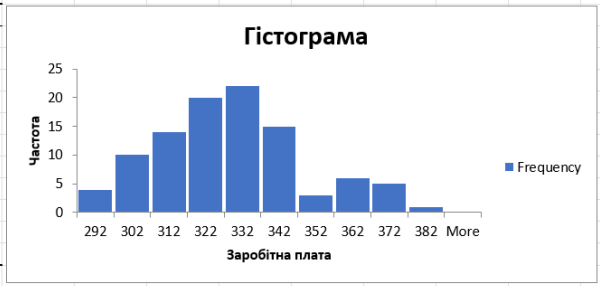


Рисунок 1 – Гістограма в Data Analysis

Серед можливостей пакету EXCEL є також описові статистики (Descriptive Statistics) а також функція побудови лінійної регресійної моделі, яка знаходиться серед статистичних функцій =LINEST. Приклад побудованої регресійної моделі показано на рисунку 2.

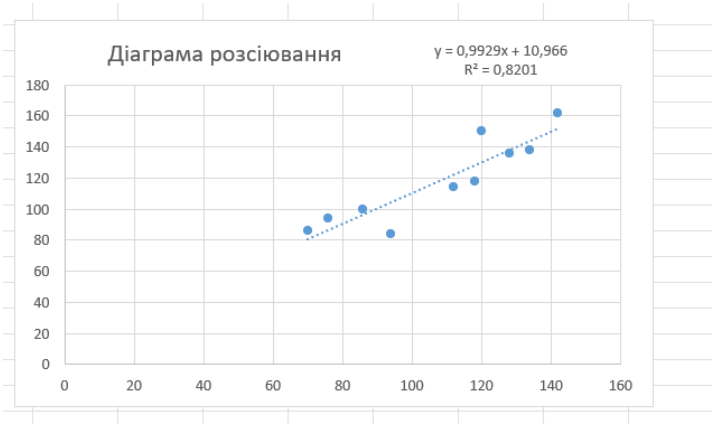


Рисунок 2 – Діаграма розсіювання

В пакеті EXCEL також є можливості реалізації однофакторного і двофакторного дисперсійного аналізу, які також знаходяться в пакеті Data Analysis, приклади реалізації наведено на рисунку 3.

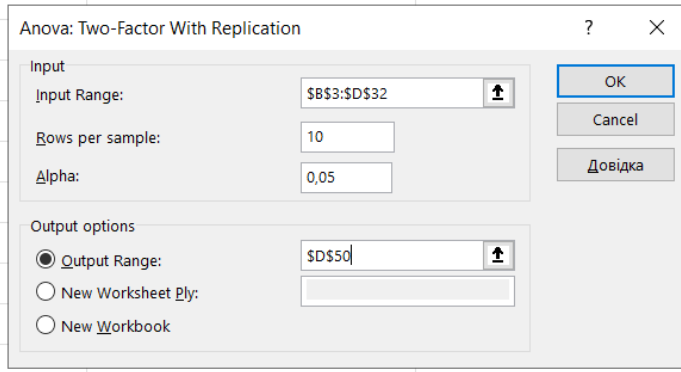


Рисунок 3 – Вікно двофакторного дисперсійного аналізу.

Як бачимо, пакет EXCEL, який є доступним для кожного користувача має потужні можливості для статистичного аналізу та візуалізації даних. На жаль в електронних таблицях Microsoft 365 такі можливості є обмеженими.

Література

1. Жлуктенко В. І., Наконечний С. І. Теорія ймовірностей і математична статистика: Навч.-метод. Посібник. У 2 ч. – Ч. 1. Теорія ймовірностей. – К.: КНЕУ, 2000 – 304 с.

2. Жлуктенко В. І., Наконечний С. І., Савіна С. С. Теорія ймовірностей і математична статистика: Навч.-метод. Посібник: У 2 ч. – Ч. 2. Математична статистика. – К.: КНЕУ, 2001. – 336 с.

3. Стасюк М.Ф., Карабин О.О., Кусій М.І. Статистичний аналіз. – Львів: ЛДУ БЖД, 2015. – 200с.

УДК 004.414

ОСОБЛИВОСТІ ФОРМУВАННЯ ПРОМПТІВ У ГЕНЕРАТИВНОМУ ДИЗАЙНІ

Жезло Н., Хлевной О.
Львівський державний університет безпеки життєдіяльності

Промпт-інжиніринг (Prompt Engineering) — це постановка конкретних запитань або передача детальної інформації генеративним інструментам штучного інтелекту (ШІ), зокрема нейромережам для створення та обробки зображень, для отримання найкращих результатів.

Із зростанням популярності генеративних інструментів штучного інтелекту для особистого та бізнес-користування хороші навички промпт-інжинірингу можуть допомогти з вашими запитами. Чим конкретнішим і детальнішим буде підказка, тим кращим буде результат.

При цьому варто розуміти, що існують різні нейромережеві продукти для генерації зображень, кожен з яких має свої переваги і недоліки. Фахівцями ресурсу Incrypted [1] було виконано порівняльний аналіз найпопулярніших генеративних нейромереж на основі виконання ними однотипних завдань – генеруванням NFT-колекції (таблиця 1)

Таблиця 1

Порівняння роботи нейромереж для генерування зображень

Критерій	Midjourney	Artbreeder	Dream.ai	Gencraft	Nightcafe	DALL-E	AI NFT Generator
Інтерфейс /зручність використання	4	2	4	4	2	4	4
Швидкість генерації	5	4	4	4	2	4	4
Якість генерації одного NFT	4	1	2	3	1	1	4
Якість генерації NFT-колекції	3	1	1	2	1	1	3
Швидкість створення NFT-колекції	3	1	1	2	1	1	2
Заміна частини зображення	2	1	1	2	1	1	2
Загальна оцінка	8/10	4/10	3/10	6/10	1/10	2/10	6/10

Як бачимо, для більшості нейромереж для генерування зображення найважчим завданням є створення серій однотипних зображень і редагування фрагментів зображень.

Проаналізуємо основні закономірності при формування промптів для у генеративному дизайні.

1. Вибір мистецького напряму або стилю. Це першочергове завданням при роботі із кожною нейромережею. При цьому можна обирати за основу як творчість конкретного художника, так і більш загальну стилізацію: кіберпанк, поп-арт, реалізм тощо. При цьому кожен продукт дає змогу експериментувати, змінюючи інтенсивність стилю (наприклад, для Midjourney це використання запиту --stylize <число від 625 до 60 000>, тоді як для Adobe FireFly — [stylize = 90,10]: числа в дужках мають дорівнювати 100, і що вище друге число, то точніше Firefly дотримуватиметься стилю запиту).

2. Корегування освітлення і кольорів (це можна здійснювати без особливих команд, використовуючи відповідні текстові формулювання: натуральне освітлення, м'яке світло, розсіювання, різкі тіні тощо).

3. Редагування формату та розміру зображення. Більшість сервісів генерують зображення квадатного формату, але формат можна змінювати, використовуючи команди (наприклад, для Midjourney підказка --ar дозволяє встановити співвідношення сторін, встановивши параметри, наприклад, --ar 3:2, а підказки --w <число> (ширина) і --h <число> (висота) дають змогу задавати розмір зображення в пікселях).

4. Встановлення деталізації. Кожен із сервісів має набір команд та підказок, за допомогою яких можна збільшувати або зменшувати деталізацію, а відтак і якість генерованих зображень. (Midjourney передбачає використання підказок --quality <число> або --q <число>, які дають системі команду знизити або збільшити якість зображення. Стандартно стоїть значення 1, але можна обрати 0.5 для пониження або 2 для підвищення).

5. Вибір кольорів. При цьому варто прописувати не тільки кольори, які мають домінувати, а й кольори, яких, за потреби, потрібно уникати.

6. Формулювання композиційних особливостей. Під такими особливостями розуміють вибір плану та ракурсу, освітлення (наприклад, крупний план, широкий ракурс, знімок згори, природне або студійне освітлення).

7. Вибір фізичних або емоційних характеристик елементів зображення (розміри, матеріали, текстури, емоції тощо).

Це, звісно, не вичерпний алгоритм побудови запитиів, який не дає гарантії стовідсоткової відповідності результатів очікуванням, але структурування запитів перевірене на практиці і дозволяє суттєво підвищити результативність використання нейромережевих ресурсів.

Література

1. 11 найкращих нейромереж для генерації зображень за описом. Створюємо NFT-колекцію за допомогою AI (готові промпти всередині) <https://incrypted.com/ua/top-nejromerej-dlja-generacii-kartynok-nft-po-opusy/> (2023, листопад, 10).

2. Як малювати в Midjourney: нейромережа малює зображення за текстовими запитами <https://cityhost.ua/uk/blog> (2023, листопад, 11).

УДК 004.032.26

НЕЙРОМЕРЕЖЕВА МОДЕЛЬ КЛАСИФІКАЦІЇ РУХІВ ЛЮДИНИ ЗА СИГНАЛОМ З IMU-СЕНСОРІВ

Жеруха Роман
Приватний заклад вищої освіти IT СТЕП Університет, м. Львів

Анотація. Інформаційні технології, в тому числі нейронні мережі, активно розвиваються в наш час. Аналогічно, Інтернет речей (IoT) також набуває поширення, зокрема завдяки прогресу в сенсорних, бездротових і мікропроцесорних технологіях. Поєднання світу Інтернету речей і досягнень в застосуванні нейромереж створюють величезні можливості, зокрема, для покращення професійної підготовки спортсменів різних видів спорту.

Ключові слова: інформаційні технології; IT; нейронні мережі; сенсори; інтернет речей; спорт.

В різних видах спорту наукові досягнення комп'ютерних наук активно застосовуються вже багато років. Наприклад, під час Чемпіонату світу з футболу 2022 використовувалась напівавтоматична технологія визначення положення офсайду. Під час останнього чемпіонату світу по футболу серед жінок 2023 використовувався м'яч з вбудованим сенсором, який передавав інформацію про кожен момент руху м'яча 500 разів на секунду.

В боксі ж, наприклад, використовується продукт «Striketec», що за допомогою сенсору відстежує рухи, які виконують руки боксера, при цьому заміряючи швидкість і силу нанесених ударів. Загалом у сфері спорту вирішуються всі основні типи задач Data Science: передбачення, прогнозування, кластирізація і класифікація.

Для сфери боксу актуальною є задача класифікації типів ударів під час проведення тренування спортсменів і порівняння ударів з досконалими ударами. Техніка, використовуючи яку спортсмени досягають найкращих спортивних результатів (техніка, яку використовують найсильніші спортсмени), вважається найбільш досконалою. Для боксу можна виділити 3 основних типів ударів: джеб, хук, крос. Автоматичне розпізнавання кожного виду ударів уможливить оцінку якості тренування спортсмена.

Пропонується розробити просту і доступну систему аналізу тренування боксерів-аматорів у формі аплікації, за допомогою якої можна б було визначати, який тип удару виконується і чи він технічно правильно виконаний. Такий застосунок можна розробити, використовуючи смартфон як пристрій, що збиратиме необхідні дані для аналізу ударів під час тренувань. Смартфони сучасних моделей містять в собі IMU-сенсори з вбудованими акселерометрами і гіроскопами – пристороями, які вимірюють лінійне і кутове прискорення. IMU (Inertional Messurment unit) - сенсори - інерційні вимірювальні пристрої, що вимірюють значення швидкості, орієнтації, та гравітаційних сил з якими рухається тіло, використовуючи для цього поєднання акселерометрів, гіроскопів.

Зчитуючи дані з смартфонів про прискорення удару в трьохвимірній системі координат, ми матимемо величину прискорення удару, що буде на-

шим джерелом даних для подальшої класифікації ударів. Задача класифікації – це задача розбиття множини об'єктів або спостережень на апріорно задані групи (класи), всередині кожної з яких вони вважаються схожими один на одного, та мають приблизно однакові властивості й ознаки.

Здійснювати класифікацію ударів на основі даних про їхнє прискорення пропонується за допомогою нейронних мереж. Нейронні мережі – це адаптивні системи для обробки та інтелектуального аналізу даних, які є математичною структурою, що імітує роботу людського мозку, демонструючи такі його властивості, як здібність до навчання, узагальнення і кластеризації інформації, здатність будувати прогнози. Нейромережі не потребують заздалегідь відомої моделі, а будують її самі на основі інформації, яку отримали.

Саме тому нейронні мережі застосовуються в тих випадках, коли вирішуються завдання прогнозування, класифікації і управління, а також в тих випадках, коли наявні задачі, які погано алгоритмізуються, і для вирішення яких необхідні або постійна робота аналітиків, або адаптивні системи автоматизації, якими і є нейронні мережі. В нашому випадку розробка нейромережевої класифікаційної моделі є необхідною частиною функціоналу мобільного додатку для боксерів-аматорів. Для навчання нейронної мережі пропонується здійснити тестову вибірку, яка буде зібрана з допомогою IMU-сенсора, вбудованого в смартфон, шляхом здійснення 10-ти тренувальних ударів кожного виду почергово обома руками в повітря декількома спортсменами. При здійсненні ударів, смартфон можна помістити в боксерську рукавицю таким чином, щоб він фактично рухався ідентично руху кулака спортсмена.

Точність моделі оцінюватиметься співвідношенням похибок True Positive, True Negative, Faulse Positive, Faulse Negative згідно Матриці невідповідностей. Якшо точність системи становитиме 95% True positive, - то точність нас задовільнить.

Таким чином, пропонований підхід дозволить пересічній людині перевіряти результати своїх тренувань без витрати додаткових коштів з допомогою смартфону.

Використання штучного інтелекту, зокрема нейронних мереж, при аналізі даних, отриманих з IMU-сенсорів дозволяє вирішувати задачу класифікації рухів спортсмена чи спортивного снаряду і спростити процес тренувань, а також допомогти суддівству при вирішенні спірних моментів за допомогою новітніх технологій. У майбутньому, використання IMU-сенсорів в поєднанні з штучним інтелектом, може спричинити бум в аналізі різних спортивних змагань, якісно покращити ефективність тренувань спортсменів і дозволить аматорам аналізувати свої рухи під час тренувань на відповідність “правильним”, еталонним рухам найкращих спортсменів

Література

1. М. Романенко. Бокс. – К., Вища школа, 1985.
2. Тимощук П.В. Штучні нейронні мережі: Навчальний посібник. – Львів : Видавництво Львівської політехніки, 2011.
3. Russell, S. J., & Norvig, P. (2009). Artificial Intelligence: A Modern Approach. Pearson.

УДК 614.8

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ДЛЯ ЗАПОБІГАННЯ НАДЗВИЧАЙНИМ СИТУАЦІЯМ

Карлінський Я.В., Оверченко М.С., Гаврись А.П.
Львівський державний університет безпеки життєдіяльності

На даний момент в країні часто застосовуються новітні технології, які допомагають виконувати різноманітні завдання з моніторингу надзвичайних ситуацій та природних катастроф швидше та безпечніше ніж це робила б людина, тому в наш час це дуже актуально та практично.

Кожному департаменту Державної служби України з надзвичайних ситуацій визначені завдання [1] для яких можуть застосовуватися технології безпілотних літальних апаратів (БПЛА).

Департамент запобігання надзвичайним ситуаціям відповідно до покладених на нього завдань може залучати БПЛА у питаннях державного нагляду (контролю) у сфері цивільного захисту, пожежної та техногенної безпеки [1, 2].

Першим завданням є моніторинг потенційно небезпечних територій. Технологія БПЛА дає можливість отримати інформацію про ситуацію в реальному часі та виявляти потенційні загрози з великих висот. Це особливо корисно при спостереженні за торфополями або зсувонебезпечними територіями, а також моніторингу стану лісового масиву в пожежонебезпечний період. Використання технології БПЛА може значно полегшити та підвищити ефективність таких операцій спостереження.

Використання БПЛА для огляду потенційно небезпечних територій дозволяє безпечно та ефективно збирати інформацію, оскільки БПЛА оснащені камерами та сенсорами, які можуть робити високоякісні знімки об'єктів на великих відстанях та з високою роздільною здатністю. Це корисно для оцінки стану інфраструктури, виявлення потенційних небезпек, як описано в роботі [3], а також у сферах, пов'язаних з навколишнім природним середовищем і безпекою.

Другим завданням для якого можна застосовувати дрони це оповіщення та інформування населення. БПЛА можуть використовуватися для попередження про надзвичайні ситуації шляхом трансляції зображень, отримання знімків з небезпечної зони і надання критично важливої інформації за допомогою високотехнологічних засобів зв'язку. Це дозволяє швидко і ефективно передавати важливі повідомлення та інструкції населенню, допомагаючи керувати евакуацією і мінімізувати ризики. Технологія БПЛА може бути невід'ємною частиною систем інформування та оповіщення на надзвичайні ситуації, сприяючи підвищенню безпеки і координації в кризових ситуаціях.

Ще одною сферою застосування є розслідування причин пожеж. БПЛА можна використовувати для розслідування причин надзвичайної ситуації або пожежі, а також для забезпечення доступу до важкодоступних або небезпечних районів. Вони оснащені камерами високої чіткості і тепловізійними камерами, які можуть надавати детальні зображення і дані, що допомагають визначити причину інциденту. Це включає визначення джерела інциденту, аналіз пошкоджень і аналіз взаємозв'язків.

Використання БПЛА в розслідуванні може значно прискорити процес і дозволити збирати інформацію швидко і об'єктивно. БПЛА можна використовувати для прогнозування ймовірності пожеж, повеней, зсувів і селів шляхом збору та аналізу даних про рослинність, геологічні параметри, погодні умови та моніторингу інших факторів.

Загалом ДСНС України можуть використовувати безпілотні літальні апарати для моніторингу виявлених небезпечних зон, інспекції об'єктів, оповіщення населення та розслідування причин надзвичайних ситуацій Використання БПЛА полегшує збір та аналіз даних і забезпечує швидке та ефективне реагування на ризики у сфері цивільного захисту, пожежної та промислової безпеки.

Література

1. Наказ ДСНС України від 20.11.2018 № 675 «Про допуск до експлуатації безпілотних літальних апаратів».

2. Havrys, A. P., Tarnavsky, A. B., Lavrivskiy, M. Z., & Veselivsky, R. B. (2017). Rationale use of unmanned aircraft technology as a means of detecting accidents and emergencies situations.

3. Гаврись, А., & Хлевной, О. (2022). Software-based method of determining the necessary population evacuation zone in case of a chemical accident. Надзвичайні ситуації: попередження та ліквідація, 6(2), 116-128.

УДК 637.5.02

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РІЗНИХ АРХІТЕКТУР ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ АНАЛІЗУ ВЕЛИКИХ ОБСЯГІВ ДАНИХ

Качмарик М.Р., Лясковська С.Є.
Національний університет «Львівська політехніка», Львів

Ця робота вивчає ефективність різних архітектур глибоких нейронних мереж, таких як DNN і TabNet, для аналізу великих наборів даних. Використовуючи CatBoost як базову лінію, він підкреслює, як вбудовані NLP підвищують точність прогнозування, зокрема в міському плануванні та аналізі короткострокових цін на оренду.

Ключові слова: глибокі нейронні мережі, великі обсяги табличних даних, обробка природної мови.

The paper examines the effectiveness of various deep neural network architectures, like DNN and TabNet, for analyzing large datasets. Using CatBoost as a baseline, it highlights how NLP embeddings enhance predictive accuracy, particularly in urban planning and short-term rental price analysis.analysis.

Key words: deep neural networks, large volumes of tabular data, Natural Language Processing.

Підвищення точності інтелектуального аналізу даних є важливою задачею в різних прикладних областях. Швидкий розвиток у сфері інтелектуального аналізу даних став вирішальним для безлічі програм. Оскільки ми перебуваємо в цифровій епосі, позначеній безпрецедентним потоком даних, попит на методи машинного навчання, які забезпечують надійність і виняткову точність у класифікації та прогнозуванні, є відчутним. Ця необхідність стала каталізатором появи гібридних аналітичних парадигм, які поєднують методи кластеризації з передовими прогнозними моделями.

У оглядовому документі [1] автори досліджують використання методів глибокого навчання в контексті аналітики великих даних. Стаття в першу чергу зосереджена на тому, як глибоке навчання може ефективно вирішувати різні важливі проблеми в цій галузі. Ці виклики включають вилучення складних шаблонів із великих наборів даних, семантичне індексування для контекстної організації даних, ефективне тегування даних, швидкий пошук інформації з великих обсягів даних і спрощення завдань, які вимагають розрізнення різних типів даних. Це дослідження підкреслює ключову роль, яку глибоке навчання відіграє в розширенні можливостей аналітики великих даних, надаючи вдосконалені рішення для складних задач аналізу та обробки даних.

У цьому дослідженні було ознайомлено із інноваційною методологію двоетапного аналізу даних, яка поєднує в собі майстерність глибокого навчання, авангардні методи кластеризації та революційні атрибути вбудо-

вування. Цей підхід стратегічно розділяє об'ємні набори даних за допомогою кластеризації, а потім використовує можливості алгоритмів DNN, TabNet і Catboost у кожному окремому кластері. Попередні випробування з використанням набору даних Airbnb Global Listings [2] — детального компендіуму списків Airbnb у великих містах світу — дали глибокі результати.

Вступний етап цього методу підкреслює корисність кластеризації для створення окремих підмножин даних. Наступний етап використовує призначені моделі для полегшення прогнозного аналізу в кожному кластері. Важливо, що засвоєння вбудованої обробки природної мови (NLP) під час навчання є ключовим, вловлюючи нюанси та складні зв'язки, поширені в текстових даних.

Робота [3] представляє детальний огляд технік обробки природної мови (NLP), особливо зосереджуючись на двох основних галузях представлення сенсу: неконтрольованому та заснованому на знаннях. У книзі розглядаються різні важливі аспекти цих технік, такі як інтерпретація, деталізація відчуттів, адаптованість до різних областей і композиційність. Зміст книги підкреслює значну роль вкладень у сфері НЛП. У ньому підкреслюється, як кодування інформації в низьковимірні векторні представлення, які можна легко інтегрувати в сучасні моделі машинного навчання, стало ключовою подією в NLP.

Порівняні результати моделювання підкреслюють ефективність розширеного методу без використання вбудованих засобів, зведено у таблиці 1.

Таблиця 1.

Model		MSE	MAE	R2 Score
CatBoost	train	80.28	47.91	0.61
	test	84.28	50.50	0.56
DNN	train	82.79	49.49	0.58
	test	84.42	50.75	0.56
Tabnet	train	88.10	54.14	0.53
	test	88.50	54.34	0.53

Після інтеграції впроваджень NLP спостерігається помітне покращення точності прогнозування, що зведено у таблиці 2.

Таблиця 2.

Model		MSE	MAE	R2 Score
CatBoost	train	70.41	41.96	0.69
	test	74.47	43.93	0.66
DNN	train	69.77	41.04	0.70
	test	72.63	42.44	0.68
Tabnet	train	78.41	47.15	0.63
	test	81.02	48.21	0.60

Після поглибленого аналізу модель DNN показує гідну похвали продуктивність, особливо за такими параметрами, як середня квадратична похибка (MSE) і середня абсолютна похибка (MAE) на етапах навчання та тестування. Результати TabNet також заслуговують на увагу, демонструючи його потенціал у прогнозних завданнях.

Застосувавши техніки NLP у всіх моделях спостерігався приріст продуктивності на 15-20%. Це було найбільш очевидно в показниках MSE та оцінки R2, де спостерігалася розширена здатність більш точно прогнозувати ціни оренди житла. Моделі не тільки виграли від зменшення помилок, але й покращення оцінки R2 також вказали на кращу відповідність моделей дисперсії даних.

Висновки

Це дослідження підкреслює можливості DNN і TabNet у розширеному аналізі даних, особливо якщо вони збагачені вбудованими NLP. У той час як DNN перевершує зв'язки складних даних, TabNet пропонує чудову інтерпретацію. Інтеграція впроваджень значно підвищує точність прогнозування, підкреслюючи їх важливу роль. Отримані результати пропонують багатообіцяючі шляхи використання таких методів у високоточних прогнозних областях.

Література

1. Bilal J., Haleem F., Murad K., Deep learning in big data Analytics: A comparative study. Computers & Electrical Engineering. — 2019 — V. 75, P. 275-287.

2. Airbnb Global Listings. [Електронний ресурс] Режим доступу: https://www.kaggle.com/datasets/joebeachcapital/airbnb (дата звернення: 15.09.2022).

3. Pilehvar M. T., Camacho-Collados J. Embeddings in Natural Language Processing: Theory and Advances in Vector Representations of Meaning. Morgan & Claypool Publishers, 2020., P. 77-8

УДК 378.351

ҐЕНДЕРНІ ОСОБЛИВОСТІ ПРОФЕСІЙНОГО СТАНОВЛЕННЯ ОСОБИСТОСТІ МАЙБУТНІХ ФАХІВЦІВ ТА ФАХІВЧИНЬ ДСНС УКРАЇНИ

Коваль Ігор
Львівський державний університет безпеки життєдіяльності

На основі теоретико-методологічного аналізу наукової літератури проаналізовано особливості ґендерної ідентичності особистості «Я-чоловік» у чоловіків і «Я-жінка» у жінок. Встановлено, що трансформації у рольовій поведінці пов'язані із деякою зміною нормативних еталонів маскулінності та фемінності.

Ключові слова: ґендерні особливості, становлення особистості, рольова поведінка, ідентичність.

On the basis of the theoretical and methodological analysis of scientific literature, the peculiarities of the gender identity of the personality "I-man" in men and "I-woman" in women were analyzed. It has been established that transformations in role behavior are associated with some change in normative standards of masculinity and femininity.

Keywords: gender characteristics, personality development, role behavior, identity.

Нова соціально-політична ситуація в Україні, що пов'язана з війною, зокрема зміною соціальних стереотипів, продукує вивчення особливостей професійного становлення особистості в галузі безпеки людини із врахуванням соціокультурного розуміння гендеру. Відповідно до Закону України «Про забезпечення рівних прав та можливостей жінок і чоловіків», особливої актуальності набуває проблема визначення чинників формування ґендерної толерантності у здобувачів вищої освіти, необхідність розроблення новітніх технологій професійної підготовки, релевантних практиці рівних прав та можливостей чоловіків та жінок.

У період цілеспрямованості всіх структур нашої держави на євроінтеграцію, інтерес до ґендерної проблеми постійно зростає, що виявляється у широкому колі науковців (Г. Бендас, Ж. Богдан, Н. Борисенко, Л. Верба, К. Гавриловська, І. Грабовська, О. Кікінеджі, П. Климчук, Л. Любіна, Ю. Малігонова, А. Мартинюк, К. Павліченко, Т. Солодовник, С. Федушко, Л. Шевченко, Р. Яремко). Ще до недавна в світі притримувались традиційних поглядів на жінку та чоловіка, тобто незважаючи на рівні права і можливості, історично визначено демінантні професії, як для одних, так і для інших, що часто впливає на вибір майбутньої професії [2; 3].

Ґендерна ідентичність особистості «Я-чоловік» у чоловіків і «Я-жінка» у жінок розуміється як частина її самосвідомості, усвідомлення себе як носія певної статі, ставлення до цього процесу, надбання певних форм поведінки, навичок, стереотипів в процесі життєдіяльності. Як підструктура самосвідомості ґендерна ідентичність виступає детермінантою особистісного самоставлення і визначає адаптаційні потенції особистості. Розвиток адаптивного типу ґендерної ідентичності продукує в індивіда високий рівень самоприйняття і задоволення життям, досягнення самоцінності і гармонії у взаємодії з навколишнім середовищем [1, с. 224].

Таким чином, сьогодні відбуваються певні трансформації у рольовій поведінці майбутніх фахівців і фахівчинь ДСНС України, що пов'язані із деякою зміною нормативних еталонів маскулінності та фемінності, що стають менш конструктивними та однозначними. Все більша кількість сучасних рятувальників та рятувальниць демонструють нові типи й моделі взаємостосунків один з одним, відповідно до яких у міжособистісній взаємодії принцип домінування й верховенства змінюється орієнтаціями на партнерство й паритет.

Література

1. Кікінежді О. М. Ґендерна ідентичність в онтогенезі особистості: монографія. Тернопіль : Навчальна книга – Богдан, 2011. 400 с.

2. 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. / МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2021. 296 с., с. 96-98.

3. Yaremko R., Vavryniv O., Tsiupryk A., Perelygina L., & Koval I. (2022). Research of content parameters of the professional self-realization of future fire safety specialists. Amazonia Investiga, 11(53), 288-297.

УДК 378.147:004.4

ВЗАЄМОДІЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ГЕЙМІФІКАЦІЇ: НОВИЙ ЕФЕКТИВНИЙ ТРЕНД СУЧАСНОЇ ОСВІТИ

Ковальчук Ірина-Надія, Смотр Ольга
Львівський державний університет безпеки життєдіяльності, м. Львів

Робота присвячена проблемі впровадження інформаційних технологій та гейміфікації у освітній процес сучасної школи.

Ключові слова: гейміфікація , інформаційна технологія, електронне навчання.

The paper is devoted to the problem of introducing information technology and gamification into the educational process of a modern school.

Keywords: gamification, information technology, e-learning.

Сьогодні інформаційні технології стали невід'ємною частиною нашого життя та відіграють значну роль у розвитку людства. У цих умовах система навчання також зазнає змін. Питання дуже актуальне у сучасному освітньому середовищі, адже якісне викладання дисциплін не може здійснюватися без використання можливостей, які надають нам комп'ютерні технології та інтернет. З екрану смартфона, ноутбука чи комп'ютера щохвилини на нас ллється величезний потік інформації, яка досить часто модифікована під гру або сприймається як така, проте це не заважає нам використовувати ігрові елементи як стимул та потенціал до саморозвитку. Сучасна система освіти відповідає технологічному прогресу. З п'яти трендів освіти, наведених журналом «Форбс» – дистанційна освіта, персоналізація, ігровізація, інтерактивні підручники, навчання через відеоігри. Як бачимо, чотири з п'яти наведених трендів освіти, належать до гейміфікації.

Гейміфіка́ція (ігровізація, геймізація, англ. gamification) — використання ігрових практик та механізмів у неігровому контексті для залучення кінцевих користувачів до розв'язання проблем [3, 4]. Гейміфікація була досліджена у декількох царинах, серед яких: взаємодія з клієнтами, виконання фізичних вправ, повернення інвестицій, пунктуальність та навчання. Більшість досліджень показали позитивні тенденції після гейміфікації. Американська ігрова дизайнерка Джейн Макґоніґал у своїй книзі «Reality Is Broken: Why Games Make us Better and How they Can Change the World» [5]. спрогнозувала, що до 2015 року ринок гейміфікації досягне $15 млрд, й вона проникне в усі сфери людської діяльності, у тому числі й в освіту.

Можемо з певністю стверджувати, що прогноз Джейни Макґоніґал справдився. Поступово процес гейміфікації (ігровізації) набув поширення в усіх сферах нашої життєдіяльності і, звісно ж, сфера сучасної освіти не стала

винятком. У 2020 році експерти компанії Growth Engineering засвідчили, що гейміфікацію використовують понад 70% компаній зі списку компаній Global 2000 та в подальшому прогнозують, що глобальний ринок гейміфікації зросте до 30,7 мільярда доларів США до 2025 року при середньорічному темпі зростання у 27,4% [6] . При цьому, на сьогоднішній день найбільше використовує гейміфіковані рішення роздрібна торгівля, займаючи 28,6% ринку, освіта ж слідує за нею як наступний за популярністю сектор .

Класичні освітні методики часто ігнорують простий, але безмежно значущій факт – навчання має приносити радість, воно має бути цікавим. Так влаштований мозок людини: коли замість боротьби з нудьгою є натхнення і позитивні емоції, інформація засвоюється краще [1].

Основна принада ігрових методик – це ставлення до помилок. Ми звикли , що за помилки завжди карають, але рідко коли вчителі чи викладачі хвалять за правильні відповіді або рішення. Фіксація на помилках призводить до того, що концентрація більше спрямована на оцінки, ніж на знання [2].

У комп'ютерних іграх, навпаки, помилки вітаються і є основним інструментом досягнення успіху. Граючи, ми знаємо, що немає нічого страшного в невдачі – чим швидше ми зробимо щось не так, тим швидше ми зможемо знайти вірне рішення.

Отже, впровадження гейміфікації допомагає мотивувати дітей і залучати їх до освітнього процесу, розвиваючи різні розумові навички. Дозволяє дітям вчитися в інтерактивному середовищі, в якому вони можуть тренуватися, робити помилки і виправляти їх.

Пандемія COVID-19 та війна в Україні суттєво вплинули на сферу освіти . Викликали зростання зацікавленості в інформаційних технологіях для навчання та навіть для того, щоб забезпечити доступ до освітніх ресурсів під час певних обмежень. А саме :

- Застосування платформ для відеоконференцій дозволило здійснювати дистанційне навчання, забезпечуючи безпеку для учнів та педагогічних працівників.
- Збільшення використання онлайн-ресурсів для навчання та самонавчання, таких як електронні підручники, відеоуроки та інтерактивні завдання.
- Застосування електронних засобів для проведення тестів та оцінювання знань, а також відстеження успішності учнів (в.ч. реформи щодо ЗНО після повномасштабного вторгнення).

Таким чином процес впровадження інформаційних технологій в освіту прискорився, але також виокремились певні проблеми пов'язані з доступністю та якістю дистанційного навчання. Сьогодні ми продовжуємо вдосконалювати нашу освіту за допомогою інформаційних технологій з елементами гейміфікації Важливо продовжувати розвивати інфраструктуру і технології для забезпечення якісної освіти в будь-яких умовах.

Література

1. Смотр О.О. *Використання інструментарію інформаційних технологій для підвищення мотивації студента до навчання у форматі змішаної освіти* / О. Смотр, М. Рашкевич, Р. Головатий, Х. Мечус // 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.

2. Любович А.А. *Сучасні інформаційні технології в освіті* / А.А. Любович, О.Г. Єсіна // інформатика та інформаційні технології: студ.наук.конф., 20 квітня 2015р. :матер.конф.– Одеса, ОНЕУ.– С. 118-120.

3. GIOS – інтерактивні курси математики [Електронний ресурс]. – Режим доступу::https://blog.gioschool.com/gamification

4. Вільна енциклопедія «Вікіпедія» [Електронний ресурс]. – Режим доступу:: https://uk.wikipedia.org/wiki/%D0%93%D0%B5%D0%B9%D0%BC%D1%96%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F

5. Jane McGonigal. Reality Is Broken: Why Games Make Us Better and How They Can Change the World. – Penguin, 20 січ. 2011 р. - 416 стор.

6. 19 GAMIFICATION TRENDS FOR 2022-2025: TOP STATS, FACTS & EXAMPLES. [Електронний ресурс]. – Режим доступу: http://www.british-legends.com/CMS/index.php/about-mud1-bl/history

УДК 004.94

ISAAC SIM: МОДЕЛЮВАННЯ ТА КОНТРОЛЬ ПОВЕДІНКИ БАГАТОМАЯТНИКОВОЇ СИСТЕМИ

Котелович Денис, Борзов Юрій
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі розглянуто можливості використання платформи Isaac Sim для моделювання та тестування алгоритмів керування багатомаятниковими системами у віртуальному середовищі.
Ключові слова: динамічна система; моделювання; маятник; симуляційне середовище; робототехніка

The paper considers the possibilities of using the Isaac Sim platform for modeling and testing control algorithms of multi-pendulum systems in a virtual environment.
Key words: dynamic system; modeling; pendulum; simulation environment; robotics

Застосування сучасних симуляційних платформ, спеціалізованих комп'ютерних програм з моделювання надає можливість суттєво збільшити можливості досліджень складних систем, інформативність отриманих результатів та внесення змін в процес моделювання. Симуляційне середовище значно спрощує процес моделювання та знімає проблему наявності достатньої інструментальної бази та вимірювальної апаратури. Крім того, у реальному вимірі часу надається можливість вносити зміни в процес моделювання, що надає безпечний і економічно ефективний спосіб тестування та оцінки складних алгоритмів керування перед їх розгортанням у реальному світі. Isaac Sim — це потужна та гнучка платформа для створення та моделювання роботів та інших складних систем. Вона дозволяє проводити високоточне моделювання складних фізичних систем і надає низку інструментів для розробки та тестування алгоритмів.

Системи з перевернутим маятником широко досліджувалися завдяки їх практичному застосуванню в робототехніці, засобах автоматизації та керування [2]. Це проста, але дуже динамічна система, яка забезпечує ідеальний тестовий стенд для контролю та аналізу стабільності. Класичним прикладом системи перевернутого маятника є маятник, прикріплений до візка, здатний рухатися по горизонтальній колії. Завдання полягає в тому, щоб підтримувати маятник у вертикальному положенні за допомогою керуючого вхідного сигналу, який переміщує візок вперед і назад уздовж колії. Ця проблема була широко досліджена в літературі та призвела до розробки широкого спектру алгоритмів керування.

Останні дослідження були зосереджені на розробці алгоритмів керування одинарних та подвійних перевернутих маятникових систем для стабілізації та виконання динамічних поворотів. Один з підходів передбачає отримання математичних моделей динаміки системи та проектування контролерів на основі цих моделей. З іншого боку, інші підходи використовують методи машинного навчання та навчання з підкріпленням, щоб забезпечувати політику контролю безпосередньо з даних. Ці підходи були успішними для досягнення стабільних вертикальних положень і виконання маневрів гойдання вгору для систем з одинарним та подвійним маятниками.

Симулятор Isaac Sim: потужний інструмент для роботизованого моделювання, який використовує формат Universal Scene Description (USD - формат тривимірного (3D) опису комп'ютерної графічної сцени) для представлення спеціальної моделі робота, включаючи фізичні характеристики та динаміку багатократного перевернутого маятника.

Isaac Sim пропонує кілька важливих функцій, які роблять його ідеальним вибором для моделювання багатомаятникових систем:

• Фізичне моделювання: Isaac Sim містить фізичний механізм, який забезпечує точне й реалістичне моделювання динаміки твердого тіла, включаючи виявлення зіткнень і реакцію.

• Симуляція давачів: середовище підтримує різноманітні давачі, зокрема камери, лідари та давачі глибини. Ці давачі можна інтегрувати в змодельовану роботизовану систему, дозволяючи контролювати на основі давачів стан багатомаятникової системи і виконувати експериментування.

• Симуляційні середовища: Isaac Sim дозволяє створювати симуляційні середовища, включаючи як фізичні макети, так і віртуальні середовища. Ця гнучкість є цінною для розробки сценаріїв, які імітують умови реального світу.

• Інтеграція з ROS2 (Robot Operating System): середовище моделювання легко інтегрується з ROS2 (вільна операційна система для програмування роботів). Ця інтеграція спрощує розробку та тестування алгоритмів керування, оскільки забезпечує основу для керування апаратними інтерфейсами та зв'язком між компонентами системи.

• Підтримка прискорення графічного процесора GPU (graphics processing unit): технологія графічного процесора GPU NVIDIA прискорює моделювання, дозволяючи ефективно моделювати складні системи. Це особливо корисно для проведення експериментів у реальному часі та швидкого створення прототипів.

• Isaac Gym: розширює можливості симулятора для підтримки експериментів RL (Reinforcement learning – навчання з підкріпленням), що дозволяють навчати політикам керування для роботизованих систем у змодельованому середовищі.

Модель багатократної перевернутої маятникової системи в Isaac Sim для дослідження ефективності алгоритму керування процесом стабілізації системи у вертикальному положенні та виконання маневрів повороту вгору представлено на рисунку 1.

Рисунок 1 – Модель для дослідження багатомаятникової системи в Isaac Sim.

Висновок: Системи з перевернутим маятником становлять складну проблему керування. Для стабілізації та виконання динамічних поворотів у багатомаятникових системах використовувалися лінійні та нелінійні алгоритми керування, а також підходи на основі машинного навчання та навчання з підкріпленням. Хоча кожен підхід має свої сильні та слабкі сторони, не існує універсального рішення для керування перевернутими маятниками. Вибір алгоритму керування залежатиме від конкретних вимог програми, таких як бажані показники продуктивності, доступні обчислювальні ресурси та параметри системи.

Література

1. 3D visualization tool for ROS. https://github.com/ros2/rviz. 2023.
2. Olfa Boubaker. “The Inverted Pendulum Benchmark in Nonlinear Control Theory: A Survey”. In: International Journal of Advanced Robotic Systems 10.5 (Jan. 2013), p. 233. DOI: 10.5772/55058.
3. Isaac Sim Extension Templates. https://docs.omniverse.nvidia.com/isaacsim/latest/advanced_tutorials/tutorial_extension_templates.html. 2023.

УДК 351/354::35.07+338.465 (477)

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНОГО СУПРОВОДУ ДІЯЛЬНОСТІ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ УКРАЇНИ В УМОВАХ ВІЙНИ

Коцюба Катерина, Твердохліб Олександр
Інститут державного управління та наукових досліджень з цивільного захисту

Законодавче забезпечення інформаційно-технологічного супроводу діяльності органів публічної влади в умовах війни заслуговує на увагу і розгляд, особливо в контексті сучасних геополітичних реалій та загроз національній безпеці держави. Сучасне нормативно-правове поле в цій галузі становить основу для гарантування захисту національного інформаційного простору та забезпечення інформаційної безпеки в умовах війни.

Сьогодні, у епоху стрімкого розвитку інформаційних технологій, інформація є важливим ресурсом та інструментом ведення війни. Вимоги до інформаційно-технологічного супроводу військових операцій стали надзвичайно високими. Це стосується не лише оборонних сил, а й усієї національної інфраструктури, у тому числі банків, систем комунікацій, енергетики та інших критичних секторів.

***Ключові слова**:* кібербезпека, інформаційний простір, інформаційна безпека, кібербезпека в умовах війни.

Закон України «Про національну безпеку» від 21.06.2018 № 2469-VIII є основоположним актом, який визначає загальні принципи забезпечення національної безпеки[1]. Він визнає необхідність захисту інформаційного простору та забезпечення інформаційної безпеки як невід'ємної частини національної безпеки, визначає інструменти та методи захисту інформації від можливих загроз.

Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII надає правовий статус кібербезпеці та вимоги до захисту критично важливих інформаційних систем [2], адже умови війни можуть призвести до збільшення кібератак та спроб порушення кібербезпеки. Цей закон встановлює правила для реагування на такі загрози та відновлення кіберінфраструктури.

Закони України, зокрема «Про національну безпеку України» і «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 80/94-ВР [3], створюють правову базу для організації інформаційно-технологічного супроводу військових операцій та забезпечення безпеки важливих інформаційних систем.

Створюються центри кібербезпеки, які мають на меті захищати від кібератак, виявляти загрози в інформаційному просторі та розробляти відповідні заходи,спрямовані на забезпечення інформаційної безпеки. Велика увага приділяється підвищенню рівня медійної грамотності серед громадян та освіті в сфері кібербезпеки, включаючи навчання виявленню та запобіганню дезінформації [5, С. 105].

Не стала винятком затверджена 26 серпня 2021 року оновлена Стратегія кібербезпеки України [6]. Це вже другий документ такого роду, затверджений за останні п'ять років.

Перша стратегія кібербезпеки України була прийнята на національному рівні в березні 2016 року і мала діяти протягом п'яти років. Документ був визнаний першим кроком у розвитку національної системи кібербезпеки України.

Прийняття Стратегії кібербезпеки України у 2016 році стало важливим кроком у запровадженні нового підходу до довгострокового планування у сфері кібербезпеки. Основний зміст цього кроку полягав в наступному:

- визначення стратегічних цілей і завдань, спрямованих на зміцнення кібербезпеки України на п'ятирічний період;
- розробка планів та стратегій впровадження нових заходів та політик у сфері кібербезпеки;
- врахування поточних загроз і ризиків у кіберпросторі та вжиття заходів для їх запобігання та усунення;
- створення основи для співпраці з іншими країнами та міжнародними організаціями в питаннях кібербезпеки.

Ухвалення нової Стратегії кібербезпеки у 2021 році свідчить про те, що робота над стратегією кібербезпеки має бути продовжена, плани актуалізовані та визначені конкретні завдання з метою подальшого посилення кіберзахисту України в умовах зростання загроз у кіберпросторі.

Нова Стратегія кібербезпеки України враховує здобуті раніше знання і виявлені проблеми, а також враховує сучасний та майбутній стан кібербезпекового середовища як на національному, так і на міжнародному рівнях. Крім того, вона враховує положення Стратегії кібербезпеки Європейського Союзу на цифрове десятиліття, а також стратегій кібербезпеки окремих держав-членів ЄС та країн-членів НАТО.

З 2022 року суттєво зросла кількість кібератак та кібератак, спрямованих на українські державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури. Основні цілі хакерів – кібершпигунство, порушення доступності державних інформаційних сервісів, знищення даних інформаційної системи. Кількість критичних атак зросла в 3,8 рази, а кількість зареєстрованих критичних кіберінцидентів зросла на 128%[7].

У другому кварталі 2023 року система виявлення вразливостей та реагування на кіберінциденти та кібератаки була дуже активною і ефективною. Всього було оброблено 3 мільярди подій, отриманих через моніторинг, аналіз та передачу телеметричних даних стосовно кіберінцидентів та кібератак. Зафіксовано 122 мільйони підозрілих подій інформаційної безпеки під час первинного аналізу, і опрацьовано 55 тисяч критичних подій інформаційної безпеки, які вважались потенційними кіберінцидентами. Відзначається збільшення кількості подій в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником», а загальна кількість критичних подій інформаційної безпеки зросла на 38,1%. У цьому контексті було виявлено декілька шкідливих програм, зокрема Agent Tesla, Snake Keylogger, SmokeLoader, Formbook та Remcos [8, С.3].

Цікаво, що впродовж другого кварталу 2023 року в Україні спостерігалася тенденція до зменшення загальної кількості кібератак, спрямованих на організації різних галузей та форм власності. Однак, найактивнішими проросійськими угрупованнями хактивістів, такими як «Народная CyberАрмия», «WE ARE BlOODNET», «Солнцепек», «Xaknet» та «NoName057(16)» було відзначено організацію 89% з усіх зафіксованих атак у цьому періоді. Основні сектори, які стали об'єктом кібератак, включають фінансовий, урядовий, медійний, енергетичний та телекомунікаційний сектори [8, С. 3].

Важливим кроком в розвитку національної кібербезпеки в умовах війни стало проведення засідання Національного Кластера Кібербезпеки в грудні 2022 року. Під час цього заходу аналізувалися ключові досягнення та прогалини у сфері кіберзахисту, обговорювалися подальші заходи для зміцнення національної системи кібербезпеки та ефективної боротьби з загрозами у кіберпросторі. Крім того, була розроблена Стратегія кібербезпеки на 2023 рік, і були затверджені перші шість професійних стандартів для нових фахівців в галузі кібербезпеки [9, С. 269].

Спостереження за розвитком даних нормативно-правових актів свідчать про те, що Україна вдосконалює свою систему інформаційно-технологічного супроводу діяльності органів публічної влади в умовах війни, враховуючи сучасні тенденції та виклики. Важливо, щоб законодавчі зміни відображали високу динаміку розвитку інформаційних технологій та нові методи виявлення загроз, що можуть виникнути в умовах війни.

Отже, законодавче забезпечення інформаційно-технологічного супроводу діяльності органів публічної влади в умовах війни в Україні має на меті забезпечити ефективний захист інформаційного простору та забезпечити національну безпеку. Постійна адаптація законодавства до нових викликів і загроз є надзвичайно важливою для забезпечення безпеки країни в умовах сучасної геополітичної нестабільності.

Умови сучасної війни перетворилися на складний ландшафт, де інформаційна битва грає ключову роль. Україна не є винятком, і, як і багато інших країн, ми стикаємося з викликами і загрозами, пов'язаними з інформаційною безпекою та використанням технологій в умовах війни.

Законодавче забезпечення інформаційно-технологічного супроводу діяльності органів публічної влади України стає дедалі важливішим у цьому контексті. Це стосується як внутрішніх справ, так і міжнародних відносин, а також забезпечення функціонування суспільства в умовах інформаційної війни. Суть інформаційної війни полягає у впливі на суспільство, політичний процес, інформаційний простір, і навіть на вибори через інформаційні кампанії, дезінформацію та кібератаки. І в умовах війни, коли країна вже зазнає фізичних агресійних дій, інформаційна безпека стає додатковою загрозою.

Одним з ключових аспектів є захист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. Вирішення цієї проблеми передбачає розробку і впровадження системи кіберзахисту, яка б дозволяла вчасно виявляти та реагувати на кіберзагрози. Крім того, необхідно регулювати використання інформаційних технологій у процесах прийняття рішень

та взаємодії з громадськістю. Це охоплює сферу відкритих даних, цифрову демократію та захист прав і свобод громадян у кіберпросторі. Завдяки правильному законодавчому забезпеченню інформаційно-технологічного супроводу, органи публічної влади зможуть ефективно захищати державні інтереси в інформаційному просторі, запобігати кіберзагрозам та дезінформації. Важливою є інтеграція цих правил і норм у міжнародні стандарти і норми, оскільки війна в інформаційному просторі не має кордонів.

Таким чином, законодавче забезпечення інформаційно-технологічного супроводу діяльності органів публічної влади України має першочергове значення, оскільки це допомагає забезпечити безпеку держави в умовах інформаційного конфлікту, національної інформаційної системи та захистити права та свободи громадян.

Література:

1. Про національну безпеку : Закон України від 21.06.2018 2469-VIII *Офіційний вісник України*. 2018. № 55 (20.07.2018).С. 1903. URL : https://ips.ligazakon.net/document/T182469.

2. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII. *Офіційний вісник України*, 2017, № 91 (21.11.2017). С. 2765. URL : https://ips.ligazakon.net/document/T172163.

3. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94. *Відомості Верховної Ради України.* 1994. № 31 (02.08.94). С. 286. URL : https://ips.ligazakon.net/document/Z008000. (дата звернення: 18.10.2023).

4. Про внесення змін до Положення про Єдину інформаційну систему соціальної сфери № : Постанова Кабінету Міністрів України від 27.10.2023 № 1130. *Урядовий кур'єр,* 2023, 11, 01.11.2023 № 219 (дата звернення: 03.11.2023).

5. Бакалінська О., Бакалінський О. Правове забезпечення кібербезпеки в Україні. Підприємництво, господарство і право. 2019. № 9. С. 100–108. (дата звернення: 17.10.2023).

6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013. (дата звернення: 20.10.2023).

7. Перун В. Зросла кількість російських кібератак і розповсюдження шкідливого програмного забезпечення. Держспецзв'язок. URL : https://lb.ua/tech/2022/11/10/535470_zrosla_kilkist_rosiyskih.html.

8. Звіт про роботу 2023. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Оперативний центр реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації україни. TLP:WHITE. 2023 (Q2). С.4. URL : https://scpc.gov.ua/api/files/a8bcaa27-ddaa-4d79-8209-e298466a416e (дата звернення: 21.10.2023).

9. Горінов П.В., Драпушко Р.Г. Сучасні виклики адміністративно-правових засад кібербезпеки україни в умовах воєнного стану. Юридичний науковий електронний журнал. № 1/2023. URL : http://lsej.org.ua/1_2023/63.pdf.

УДК 681.3

ОРГАНІЗАЦІЯ БАЗ ДАНИХ В ПРОЕКТАХ СТВОРЕННЯ БЕКЕНД СЕРВІСІВ

Кошелєв Максим, Райта Діана
Львівський державний університет безпеки життєдіяльності, м. Львів

Обговорено важливість організації баз даних для ефективного функціонування бекендів, особливості вибору структури БД, стратегії масштабування та оптимізації. Наголошено на використанні різних типів БД для різних потреб та застосуванні архітектурних патернів для створення стійких та продуктивних систем. Розглянуто аспекти безпеки, резервного копіювання та архітектурних рішень для ефективної взаємодії бекенду з іншими системами.
Ключові слова: база даних, бекенд, інформаційні технології.

Discussed the importance of organizing databases for the efficient functioning of backends, specifics in choosing the database structure, scaling strategies, and optimization. Emphasized the use of different database types for various needs and the application of architectural patterns to create robust and productive systems. Examined aspects of security, backup procedures, and architectural solutions for the effective interaction of the backend with other systems.
***Keywords*:** database, backend, information technologies

Організація баз даних в проектах створення бекенд сервісів є ключовою складовою для успішної розробки та функціонування програмних рішень. Бекенд сервіси забезпечують обробку даних, логіку та взаємодію з фронтендом або іншими системами через API[1]. Ефективна організація баз даних у бекенді є важливою для забезпечення швидкості, надійності та масштабованості системи. Основні аспекти організації баз даних в цьому контексті включають вибір підходящої структури бази даних (реляційні БД, нереляційні БД, NoSQL), проєктування оптимальних таблиць та зв'язків між ними, нормалізацію даних для уникнення дублювання та підвищення ефективності, розробку відповідних запитів для отримання необхідної інформації та забезпечення безпеки даних.

Важливо також розглядати вибір системи управління базами даних (СУБД), яка найкраще відповідає потребам конкретного проекту, використовувати методи захисту даних та резервного копіювання для запобігання втрати інформації. Усе це сприяє підвищенню ефективності роботи бекенду, забезпечує швидкий доступ до даних та забезпечує стійкість системи у випадку навантажень або непередбачених ситуацій.

Організація баз даних в контексті створення бекенд сервісів також включає аспекти масштабованості та оптимізації. При розвитку проекту

важливо планувати на майбутнє, розглядаючи потреби в збільшенні обсягу даних та виконання більш складних операцій. Зокрема, в масштабуванні баз даних важливо враховувати можливість горизонтального та вертикального масштабування, щоб система могла ефективно працювати при зростанні обсягів інформації або навантажень.

Оптимізація баз даних також включає аналіз та вдосконалення запитів до бази даних, індексацію [2, 3] та кешування для поліпшення швидкодії системи. Це дозволяє забезпечити оптимальну роботу навіть у випадку великої кількості одночасних запитів. Залежно від потреб проекту, можна також розглянути використання різних типів баз даних для різних цілей, наприклад, графові бази даних для збереження зв'язків між даними або колоночні бази даних для оптимізації аналітичних запитів. Розробка бекенду також означає роботу зі зв'язком між бекендом і фронтендом, тому важливо розглядати архітектурні вирішення, які сприяють ефективній взаємодії між цими двома частинами системи.

Розробка бекенду також вимагає уваги до аспектів резервного копіювання та відновлення даних. Важливо мати механізми резервного збереження, що дозволяють відновлювати інформацію в разі аварійних ситуацій або втрати даних. Додатково, розробка бекенду включає розгляд архітектурних паттернів, таких як Microservices або Serverless, що можуть бути корисними для побудови гнучких, масштабованих та підтримуваних систем. Архітектурні принципи, такі як розподілені системи та використання кешування, також можуть знайти своє застосування у вирішенні проблем ефективності та швидкодії. Не менш важливим є врахування принципів безпеки, включаючи захист від несанкціонованого доступу, шифрування даних та використання методів аутентифікації та авторизації для забезпечення конфіденційності та цілісності інформації.

Література:

1. Бурак Н. Є. Модель проектно-інформаційного середовища покращення підготовки рятувальника в ментальному просторі ІТ-технологій. Вісник Львівського державного університету безпеки життєдіяльності. Львів, 2014. № 10. С. 24-32.

2. Борзов Ю. Особливості застосування комп‘ютерного моделювання для покращення навчального процесу / Ю. Борзов, Р. Головатий, Я. Магеровський. // Інформаційні технології розвитку змісту освіти. – 2019. – С. 80–81.

3. Зачко О.Б., Головатий О.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.

УДК: 378.02

ЗАСТОСУВАННЯ ІТ В ОСВІТІ

Круликівський Б.Р., Борзов Ю.О.
Львівський державний університет безпеки життєдіяльності

Розглянуто роль сучасних інформаційних технологій та можливості дистанційного навчання. Проведено аналіз ресурсів для забезпечення онлайн навчання.

Ключові слова: сучасних інформаційних технологій, інформаційно-комунікаційні технології, мобільність, електронний підручник

The role of modern information technologies and the possibility of distance learning are considered. An analysis of resources for providing online training was carried out.

Keywords: modern information technologies, information and communication technologies, mobility, electronic textbook

Сучасна інформаційна технологія (СІТ) в освіті – це комплекс навчальних і навчально-методичних матеріалів, технічних та інструментальних засобів техніки навчального призначення, а також система наукових знань про роль і місце обчислювальної техніки в навчальному процесі, про форми і методи їх застосування для вдосконалення праці викладачів та студентів.

Інформатизація суспільства пов'язана, насамперед, з розвитком комп'ютерної техніки, різноманітного програмного забезпечення, глобальних мереж (Інтернет), мультимедійних технологій.

Виникнення та розвиток інформаційного суспільства припускає широке застосування інформаційно-комунікаційних технологій в освіті, що визначається багатьма чинниками.

Інформаційно-комунікаційні технології або ІКТ – засоби, пов'язані зі створенням, забезпеченням, передачею, обробкою і управлінням інформації. Цей широко вживаний термін включає в себе всі технології, що використовуються для спілкування та роботи з інформацією. Концепція інформаційних технологій була додана до елементу комунікації і виникла у 1980-ті роки. Наразі ІКТ включають апаратні засоби (комп'ютери, сервери, тощо) та програмне забезпечення (операційні системи, мережеві протоколи, пошукові системи, тощо). Їхні можливості широко застосовують під час навчального процесу, звідси ІКТ можна вважати педагогічною технологією. Будь-яка педагогічна технологія – це інформаційна технологія, оскільки основу технологічного процесу складає отримання і перетворення інформації.

Використання сучасної інформаційної технології дає можливість розкрити гуманітарний потенціал природних дисциплін, пов'язання із формуванням наукового світогляду, розвитком аналітичного та творчого мислення, суспільної свідомості та свідомого ставлення до оточуючого світу.

Можливість навчатися в будь-якому місці. Студенти можуть вчитися, не виходячи з дому чи офісу, перебуваючи в будь-якій точці світу. Щоб

приступити до навчання, необхідно мати комп'ютер з доступом в Інтернет. Відсутність необхідності щодня відвідувати навчальний заклад – безсумнівний плюс для людей з обмеженими можливостями здоров'я, для проживаючих в важкодоступних місцевостях, які відбувають покарання в місцях позбавлення волі, батьків з маленькими дітьми.

Мобільність. Зв'язок з викладачами, репетиторами здійснюється різними способами: як on-line, так і off-line. Проконсультуватися за допомогою електронної пошти іноді ефективніше і швидше, ніж призначити особисту зустріч при очному або заочному навчанні.

Під час вивчення курсу з дисципліни «Комп’ютерна схемотехніка та архітектура компютера» ми використовуємо програму Multisim компанії розробника National Instruments для забезпечення проведення лабораторного практикуму. На заняттях з об’єктно-орієнтованого програмування ми навчаємося програмувати мовою Java використовуючи інтегроване середовище розробки IntellijIDEA. За допомогою програми Cisco Packet Tracer ми моделюємо мережі, також ця ппрограма дозволяє експериментувати з поведінкою мережі і оцінювати можливі сценарії.

Електронний підручник – це автоматизована навчальна система, що включає в себе дидактичні, методичні та інформаційно-двійкові матеріали з навчальної дисципліни, а також програмне забезпечення, яке дозволяє комплексно використовувати їх для самостійного отримання та контролю знань. Дистанційна освіта – це гнучка адаптивна модульна технологія навчання. Вона орієнтована на споживача і спирається на сучасні інформаційні та комунікаційні технології, вважається економічно-ефективною.

Один із сучасних шляхів інтенсифікації та оптимізації навчального процесу є інформатизація освіти, і зокрема, використання комп’ютерних технологій. Як показує аналіз, більшість студентів уже на ранніх стадіях навчання прекрасно усвідомлюють необхідність застосування новітніх інформаційних технологій у своїй професійній діяльності.

Гарним прикладом може бути віртуальний університет Львівського державного університету безпеки життєдіяльності.

Це навчальне середовище надає змогу відстежувати поточну успішність з дисциплін, проходження тестів, опрацювання лекційного матеріалу. Віртуальний університете є чудовим помічником для самостійного опрацювання матеріалів, які зазначені курсом.

Електронний підручник має багато переваг порівняно зі звичайним паперовим підручником. Електронні підручники були спочатку розроблені для організації дистанційної освіти. Проте, з часом, завдяки своїм можливостям навчання вони переросли в цю сферу застосування. Для того щоб електронний підручник став популярним, він повинен бути універсальним, тобто однаково придатним як для самоосвіти, так і для стаціонарного навчання, повним за змістом, високо інформативним, талановито написаним і добре оформленим.

Однак, дистанційна освіта не підходить для розвитку комунікабельності. При дистанційному навчанні особистий контакт студентів один з одним і з викладачами мінімальний, а то і цілком відсутній. Тому така форма навчання не підходить для розвитку комунікабельності, впевненості, навичок роботи у команді.

У зв'язку із теперішньою ситуацією у країні дистанційне навчання має великі перспективи, тому що виправдовує себе і є дійсно зручним. Дана форма навчання інноваційна, але вже зараз дистанційне навчання набуває своїх послідовників. Система дистанційного навчання побудована з урахуванням всіх тонкощів і нюансів, щоб забезпечити максимальну ефективність і користь навчання і в той же час, забезпечити зручність її використання.

Література

1. https://core.ac.uk/download/pdf/147039123.pdf
2. Биков В. Ю. Дистанційне навчання в країнах Європи та США і перспективи для України
3. Борзов Ю.О. Застосування комп'ютерного моделювання для забезпечення навчального процесу, Борзов Ю.О., Малець І.О., Малець Р.Б. Збірник наукових праць V Міжнародної науково-практичної конференції. – Львів: ЛДУБЖД, 19-20 жовтня 2017. – С.198-202.

УДК 004.932

ЧИННИКИ ВПЛИВУ НА ЯКІСТЬ ЗОБРАЖЕННЯ, ОТРИМАНОГО ЗА ДОПОМОГОЮ ЛІДАРА ПІД ЧАС ПОШУКОВИХ РОБІТ

Кузик О.А.
Львівський державний університет безпеки життєдіяльності

Для проведення пошукових робіт, зокрема в умовах недостатньої видимості (задимлення, туману), використання лідарів, які працюють у інфрачервоному діапазоні хвиль, дає можливість ідентифікації об'єктів. Проте за недостатньої видимості на зображенні, яке фактично є картою рельєфу, окрім об'єктів спостерігаються точки та неіснуючі об'єкти, зумовлені відбиттям та розсіюванням лазерного променя від молекул середовища. Для фільтрування зображення від хибних об'єктів потрібно встановлювати максимальну та мінімальну межі очікуваної відстані до реальних об'єктів та методи покращення якості зображення. Якість зображення погіршується із зростанням відстані та наближенні до краю зображення від центра кадру. Тому потрібно застосовувати адаптивні методи та алгоритми покращення якості зображення, які змінюють ступінь покращення залежно від місця розташування об'єктів на зображенні.

Ключові слова: лідар, рельєфне зображення, покращення зображення, умови недостатньої видимості

Лідар – це пристрій для сканування лазерним променем простору та одночасного вимірювання відстані до об'єктів. Принцип його роботи дає можливість будувати рельєфне зображення частини простору, яка сканується. За відсутності перешкод на зображенні відображаються найбільш віддалені точки об'єктів, на які потрапляє лазерний промінь. У випадку розміщення об'єктів на віддалі від фонової поверхні, на ній спостерігається їхня тінь. Також у випадку потрапляння в кадр гладких поверхонь, розташованих під гострим кутом до лазерного променя (підлога, стіна, поверхні меблів, водяна поверхня та ін.) можуть виникати дзеркальні відображення об'єктів, спричинені відбиттям прямого і відбитого лазерного променя під час сканування. У випадку наявності перешкод на шляху лазерного променя, зумовлених умовами недостатньої видимості (дим, полум'я, водяна пара, туман, пил та ін.) вимірювання відстані внаслідок відбиття від молекул перешкоди або розсіювання буде ускладненим або й неможливим. Для точок зображення, які розташовані поруч, під час сканування може фіксуватися декілька відстаней: від об'єктів, від молекул перешкоди. Тоді потрібно відділити хибні значення від істинних відстаней до об'єктів. Для цього в процесі обробки зображення потрібно відкинути зайві значення, залишаючи реальні відстані до об'єктів. Для цього окремі точки зображення потрібно відкинути. Це призведе до погіршення якості зображення об'єктів. А внаслідок розсіюван-

ня окремі точки зображення об’єктів можуть бути зміщені. Це також призводить до спотворення та зниження чіткості зображення.

Послідовність процесу обробки інформації, отриманої від лідара, зображено на рис. 1.

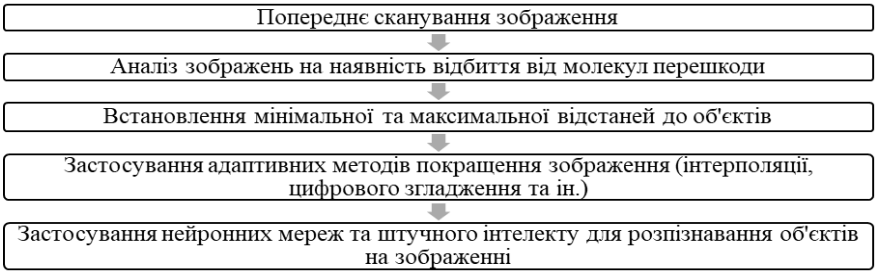


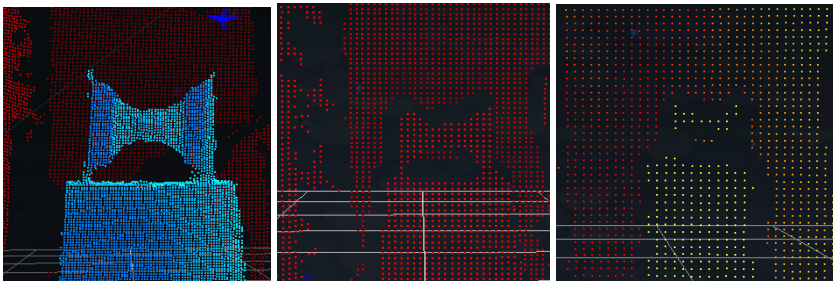
Рисунок 1 – Схема процесу обробки зображення, отриманого за допомогою лідара

Для відкидання хибних значень відстаней потрібно встановити мінімальну та максимальну відстані до об’єктів. Але ці значення наперед невідомі та можуть змінюватися за значної нерівномірності рельєфу, наявності об’єктів перед фоном, які підлягають відображенню та ін. Цей процес потрібно постійно контролювати та коригувати, оцінювати якість отриманого зображення. Наступним етапом доцільно застосовувати методи та алгоритми покращення якості зображення (інтерполяції, цифрового згладжування та ін.). Якщо проводиться пошук об’єктів наперед відомих типів та форми, тоді доцільно застосовувати нейронні мережі, провівши попереднє «навчання», або «штучний інтелект».

Використання лідара, на відміну від оптичної камери, має певні особливості отримання зображень, зумовлені різними відстанями до поверхні об’єктів у межах кадру зображення. Вони полягають у збільшенні площі точки, яка підсвічується лазерним променем, із збільшенням відстані внаслідок збільшення ширини лазерного променя. Це призводить до того, що більш віддалені точки поверхонь об’єктів будуть більшими за площею, що погіршить чіткість зображення. Це потребує застосування адаптивних методів та алгоритмів покращення якості зображення, які полягають у більшому ступені покращення якості зображення в деякому околі для віддалених фрагментів поверхонь і меншому ступені покращення якості (або взагалі не покращуючи його) для фрагментів, розташованих ближче. Такий же підхід застосовується також і для фрагментів на краях зображення та посередині.

Для оцінювання необхідності застосування адаптивного методу покращення якості зображення для об’єктів, розташованих на різних відста-

нях проведено експериментальне дослідження. Використано Intel RealSense LiDAR Camera L515 та програмне забезпечення Intel® RealSense™ Viewer [1]. Оцінювання якості зображення, отриманого за допомогою лідару проводили на відстанях 1, 2, 3, 4 та 5 м, розташовуючи спеціально виготовлену тестову рельєфну мішень з висотою 20 см, шириною 22 см та перепадами висот 1-3 см. Мішень розташовували в центрі кадру зображення (рис. 2), а також з лівого та правого країв.



а б в

Рисунок 2 – Оцінювання чіткості зображення, отриманого за допомогою лідара за допомогою мішені, розміщеної по центру на відстанях а – 1 м, б – 3 м, в – 5 м

Проаналізувавши отримані зображення, виявлено, що рельєф мішені видно лише на відстані 1 м. Із збільшенням відстані спостерігається зменшення розмірів та погіршення якості зображення. На відстанях 1, 2, 3, 4 і 5 м розміри мішені становлять, відповідно, 47×50, 22×24, 14×15, 10×11 та 5×8 пікселів. Спостерігається також певне погіршення якості зображення для тієї ж відстані із зміщенням до краю кадру зображення.

Висновки. Недостатня видимість призводить до погіршення якості зображення, спричиненого вимірюванням відстаней як від об’єктів, так і від молекул середовища, крізь яке відбувається сканування. Якість зображення погіршується із зростанням відстані до поверхні об’єктів та відхиленням від центра зображення. Для покращення якості зображення, отриманого за допомогою лідара, потрібно застосовувати як традиційні методи так і адаптивні, у яких рівень покращення залежить від відстані.

Література

1. Intel® RealSense™ LiDAR Camera L515 [Електронний ресурс]. URL: https://www.intelrealsense.com/lidar-camera-l515/.

УДК 004.412

НЕЛІНІЙНА РЕГРЕСІЙНА МОДЕЛЬ ДЛЯ ОЦІНЮВАННЯ РОЗМІРУ ВЕБ-ЗАСТОСУНКІВ, ЩО СТВОРЮЮТЬСЯ З ВИКОРИСТАННЯМ ФРЕЙМВОРКУ REACT

Кузнецов Олексій, Фаріонова Тетяна, Ворона Михайло
Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв

Анотація. В роботі на основі нормалізючого перетворення у вигляді десяткового логарифму побудовані однофакторна та двофакторна нелінійні регресійні моделі для оцінювання розміру веб-застосунків, які створюються на основі фреймворку React, з використання метрик програмного коду кількості класів та кількості методів на клас
Ключові слова: веб-застосунки, нелінійна регресійна модель, логарифмічне перетворення, React.

Abstract. In this work, based on the normalization transformation in the form of a decimal logarithm, one-factor and two-factor nonlinear regression models are built for estimating the size of web applications that are created on the basis of the React framework, using the metrics of the software code of the number of classes and the number of methods per class.
Keywords: web applications, nonlinear regression model, logarithmic transformation, React.

Створення вебзастосунків є одним з найбільш актуальних та затребуваних напрямків в галузі інженерії програмного забезпечення. Варто зазначити, що сучасна веб-розробка невід'ємно пов'язана із використанням різноманітних фреймворків. Фреймворк React є найпопулярнішим вибором серед засновників стартапів, використовується розробниками для створення програмного забезпечення, яке добре працює як на Android, так і на iOS. Підприємці віддають перевагу розробці на React, оскільки він сприяє підвищенню конверсії, надає можливість перевірки зворотних посилань, знижує витрати на розробку та підвищує впізнаваність бренду.

Побудова математичної моделі для оцінювання розміру вебзастосунків є важливим завданням веб-розробки [1]. В першу чергу, така модель надає можливість передбачити обсяг роботи, необхідний для успішної реалізації програмного проєкту, допомагає визначити його ресурси, бюджет і терміни. По-друге, оцінка розміру веб-застосунку корелює з оцінкою трудомісткості та людино-годинами, необхідними для розробки.

Існують різні визнані математичні моделі, такі як COCOMO (Constructive Cost Model) та модель Function Point Analysis. Однак, в сучас-

ному веб-середовищі, з його викликами та технологічними тенденціями, такі моделі не дозволяють врахувати всі аспекти та інновації, такі як використання сучасних фреймворків [2]. Таким чином, застосування існуючих алгоритмічних моделей для оцінювання вебзастосунків на основі фреймворку React, може призводити до низької достовірності такого оцінювання. Отже, побудова регресійної моделі для оцінювання розміру вебзастосунків, що створюються на основі фреймворку React, є актуальною задачею.

Метою роботи є розробка нелінійних регресійних моделей для оцінювання розміру веб застосунків, що створюються з використанням фреймворку React, на основі метрик програмного коду, а саме кількості строк коду, кількості класів та кількості методів на клас, що дозволить підвищити достовірність відповідного оцінювання.

Для побудови нелінійних регресійних моделей авторами зібрано емпіричні дані на інтернет-ресурсі GitHub, з проектів з відкритим кодом. Було відібрано 50 проектів з розробки веб-застосунків, що створюються за допомогою мови JavaScript та фреймворку React. Для кожного з проектів були визначені метрики програмного коду, такі як кількість рядків коду в тисячах Y, (KLOC), кількість класів X_1 та кількість методів на клас X_2 [3]. Параметри X_1 та X_2 були перевірені на предмет мультиколінеарності за допомогою коефіцієнтів впливу дисперсії (VIFs), значення яких вказують на відсутність мультиколінеарності.

На основі отриманих метрик були побудовани однофакторна регресійна модель (1)

$$Y = \widehat{b_0} + \widehat{b_1}X_1 + \varepsilon \tag{1}$$

та двофакторна лінійна регресійна модель (2)

$$Y = \widehat{b_0} + \widehat{b_1}X_1 + \widehat{b_2}X_2 + \varepsilon, \tag{2}$$

де $\widehat{b_0}$, $\widehat{b_1}$, $\widehat{b_2}$, – оцінки параметрів, ε – випадкова величина з нормальним розподілом. Після перевірки нульової гіпотези про нормальність розподілу ε за допомогою критерію Пірсона. На рівні значності 0.05 гіпотеза була відхилена. Тому, розподіл ε є негаусівським, що вказує на відсутність теоретичного обгрунтування для використання лінійної регресійної моделі. Таким чином, рекомендується побудувати нелінійні регресійні моделі (3) та (4).

$$Y = 10^{\varepsilon+\widehat{b_0}} X_1^{\widehat{b_1}} \tag{3}$$

$$Y = 10^{\varepsilon+\widehat{b_0}} X_1^{\widehat{b_1}} X_2^{\widehat{b_2}} \tag{4}$$

В якості нормалізуючого перетворення вихідних даних авторами використано одновимірне нормалізуюче перетворення у вигляді десяткового логарифму

Оцінки параметрів моделей отримані за допомогою методу найменших квадратів. Моделі (3) та (4) були побудовані із врахуванням наявності викидів за даними. Для виявлення викидів використовувалися такі методи, як квадрат відстані Махаланобіса, критерій Пірсона та критерій Фішера [4]. Порівняльні результати якостей однофакторної та двуфакторної моделей за критеріями R^2, MMRE та PRED(0,25) наведені у таблиці 1.

Таблиця 1. Показники оцінювання якості моделей

Модель	R^2	MMRE	PRED (0,25)
Однофакторна	0,34	0,46	0,30
Двофакторна	0,83	0,20	0,68

З отриманих результатів, можна зробити висновок, що двофакторна модель має кращі показники якості, ніж однофакторна модель. Однак за показником PRED (0,25) її якість не задовільна. Тому перспектива подальших досліджень полягає в удосконалені багатофакторної нелінійної регресійної моделі для оцінювання розміру веб застосунків, що створюються з використанням фреймворку React, за рахунок застосування більш складних нормалізуючих перетворень Джонсона та розробці програми, яка дозволить користувачам отримувати прогноз кількості рядків коду веб-застосунку на основі метрик кількість класів та кількість методів. Ця програма може бути використана розробниками та менеджерами проектів для оцінки ресурсів, необхідних для розробки веб-застосунків.

Література

1. Briand L.C. Property Based Software Engineering Measurement / L.C. Briand, S. Morasca, V.R. Basili // IEEE Transaction on Software Engineering. – 2009. – Vol. 22, no. 1. – p. 68–86

2. Управління проектами по створенню програмного забезпечення [Електронний ресурс]. URL: https://project.dovidnyk.info/index.php/home/upravlenieproektamiposozdaniyuprogrammno goobespecheniya/130-modelocenkistoimostisosomo

3. Software Engineering | Project size estimation techniques [Електронний ресурс]. URL: https://www.geeksforgeeks.org/software-engineering-project-size-estimation-techniques/

4. Регресійна статистика. Парна лінійна регресія: Статистичний аналіз моделі [Електронний ресурс]. URL: https://bumotors.ru/uk/regressionnaya-statistika-parnaya-lineinaya-regressiya-statisticheskii-analiz-modeli.html

УДК 004.4: 004.896

МОНІТОРИНГ ТА АНАЛІЗ ВЕЛИКИХ ОБСЯГІВ ДАНИХ ЗАСОБАМИ ПЛАТФОРМИ ELASTIC STACK

Купріков Микита, Смотр Ольга
Львівський державний університет безпеки життєдіяльності, м. Львів

Робота присвячена дослідженню ефективності використання засобів платформи Elastic Stack в розрізі моніторингу та аналізу великих обсягів даних, з метою адміністрування систем, аналізу їх безпеки, швидкодії, відмов тощо. На підставі проведеного дослідження зроблені рекомендації щодо доцільності використання платформи Elastic Stack, для вирішення завдань аналізу великих обсягів даних, моніторингу систем, логування, пошуку і аналітики великих даних

Ключові слова: платформи моніторингу та аналізу великих даних, Elastic Stack, Big Data, .

The paper is devoted to the study of the effectiveness of using the Elastic Stack platform tools in the context of monitoring and analysing large amounts of data, with the aim of administering systems, analysing their security, performance, failures, etc. Based on the study, recommendations are made on the feasibility of using the Elastic Stack platform to solve the problems of analysing large amounts of data, monitoring systems, logging, searching and analysing big data

Keywords: Big data monitoring and analysis platforms, Elastic Stack, Big Data.

Важливість роботи: В сучасному світі великі обсяги даних є необхідністю для багатьох організацій та підприємств у різних сферах. Аналіз цих даних є важливим етапом у визначенні стратегії розвитку та прийнятті ефективних управлінських рішень. Особливо актуальним на сьогодні є питання моніторингу та аналізу даних в сфері розробки та адміністрування систем безпеки даних. У зв'язку з цим, важливим завданням є вибір платформи, що значно спростить та забезпечить ефективний моніторинг та аналіз великих обсягів даних лог-файлів.

Ось деякі з найбільш популярних платформ для моніторингу та аналізу великих даних на сьогодні:

1. ***Elastic Stack:*** – раніше відомий як ELK Stack, - це набір відкритих додатків для збору, обробки, зберігання та візуалізації лог-даних.

2. ***Grafana***: – платформа візуалізації та моніторингу, яка дозволяє створювати графіки, діаграми та панелі для різноманітних джерел даних, включаючи Elasticsearch, Prometheus та інші.

3. ***InfluxDB***: – база даних для зберігання та візуалізації часових рядів даних, що використовується для моніторингу та аналізу.

4. ***Graylog***: – система управління журналами та аналізу, яка дозволяє збирати, індексувати та аналізувати журнали з різних джерел.

5. ***Datadog***: – хмарна платформа для моніторингу та аналізу даних, яка надає різноманітні інструменти для візуалізації та аналізу метрик, лог-файлів тощо.

6. ***Nagios***: – система моніторингу, яка використовується для відстеження стану різних компонентів системи та відправки сповіщень в разі проблем.

Кожна з них має свої переваги та обмеження. Вибір між цими платформами залежить від особливостей та потреб вашої організації та від конкретних вимог вашого проєкту, Однак, в контексті моніторингу та аналізу великих обсягів даних, з метою адміністрування систем та аналізу їх безпеки платформа Elastic Stack грає ключову роль, забезпечуючи потужні інструменти для збору, зберігання, обробки та аналізу даних лог-файлів.

Представлення продукту: Elastic Stack є однією з найпопулярніших відкритих платформ для обробки та аналізу великих обсягів даних. Вона включає в себе декілька ключових компонентів, які спільно працюють для забезпечення повного циклу обробки даних, від їхнього збору до аналізу.

1. ***Elasticsearch:*** Це потужний та масштабований пошуковий двигун, який дозволяє ефективно зберігати, швидко знаходити та аналізувати великі обсяги даних. Elasticsearch володіє розподіленою архітектурою, що дозволяє легко масштабувати систему залежно від обсягу даних.

2. ***Logstash*:** Цей компонент відповідає за збір, обробку та передачу різноманітних типів даних до Elasticsearch. Він забезпечує можливість фільтрації та перетворення даних перед їхнім зберіганням, що робить його незамінним інструментом для обробки журналів, подій та інших структурованих даних.

3. ***Kibana:*** Це потужний інструмент для візуалізації та аналізу даних, який дозволяє користувачам створювати динамічні та інтерактивні графіки, дашборди та звіти на основі даних, збережених у Elasticsearch. Він дозволяє швидко здійснювати пошук, фільтрацію та візуалізацію даних за допомогою простого та інтуїтивно зрозумілого інтерфейсу.

4. ***Beats:*** Це набір легких агентів, які використовуються для збору різноманітних типів даних з різних джерел. Beats дозволяє зручно збирати дані з логів, метрик системи, мережі та аудиту, що робить його універсальним інструментом для забезпечення повного збору даних для подальшого аналізу.

Ось деякі переваги та недоліки Elastic Stack у порівнянні з іншими платформами:

Переваги Elastic Stack:

- ***Гнучкість і розширюваність***: Elastic Stack дуже гнучкий і дозволяє адаптуватися до різних сценаріїв великих даних. Elasticsearch легко масштабується горизонтально, дозволяючи обробляти великі обсяги даних.

- ***Легкість використання і спрощений сетап***: Elastic Stack відомий своєю простотою у встановленні та налаштуванні. У порівнянні з іншими рішеннями, він може бути швидко розгорнутий та використаний.
- ***Широкий функціонал Kibana***: Kibana надає розширені інструменти візуалізації та аналізу даних. Він простий у використанні і дозволяє легко створювати різноманітні графіки та діаграми.
- ***Активна спільнота і підтримка***: Elastic Stack користується великою та активною спільнотою, що важливо для розвитку та вирішення проблем.
- ***Широкий набір інтеграцій***: Elastic Stack має багато готових агентів (Beats) для різних типів даних, а також інтеграцію з іншими системами.

Недоліки Elastic Stack:

- ***Витрати ресурсів при великих обсягах даних***: При обробці дуже великих обсягів даних Elastic search може вимагати значних ресурсів.
- ***Складність підтримки***: Зі збільшенням масштабів виробництва, конфігурація та підтримка може стати складнішою, особливо для не досвідчених користувачів.

Розробка та дослідження системи моніторингу та аналізу великих обсягів даних за допомогою платформи Elastic Stack відкриває шлях до ефективного управління даними та забезпечення швидкого та точного аналізу для прийняття важливих рішень. Її ефективність та гнучкість надає змогу організаціям з легкістю впроваджувати складні рішення аналітики даних для вирішення різноманітних завдань у сфері бізнесу та технологій.

Література

1. Gormley, Clinton, and Zach Davis. "Elasticsearch: The Definitive Guide." O'Reilly Media, Inc., 2015.

2. Kordunova, Y., Feltynowski, M., Prydatko, O., & Smotr, O. (2023). Математичне моделювання процесу розробки спеціалізованих програмних систем безпеко-орієнтованого спрямування. Вісник ЛДУ БЖД, 27, 23-31. https://doi.org/https://doi.org/10.32447/20784643.27.2023.03

3. Radu, Marius, "Elastic Stack for Monitoring, Logs and Metrics." Apress, 2017.

4. Elastic N.V., "Elastic Stack Documentation." - [Електронний ресурс]. – Режим доступу : https://www.elastic.co/guide/index.html

УДК 66.02+54-3

ВИДИ ЗАХИСНИХ ПОКРИТТІВ

Липовий Арсен
Українська академія друкарства, м. Львів

У роботі представлений опис видів захисних покриттів та відповідні можливості їх застосування для захисту

Плівка, покриття, поліестер, відбивання, видимість.

The paper presents an overview of the types of protective coatings and the corresponding possibilities of their application for protection.

Lamina, coating, polyester, reflection, visibility.

На теперішньому етапі розвитку засобів захисту інформації захист оптико-електронного каналу витоку інформації забезпечується здебільшого активними засобами. Однак такі засоби мають ряд недоліків, і не завжди здатні забезпечити надійний захист, тому ефективним є поєднання активних та пасивних методів. Саме тому актуальним є розроблення і застосування оптично прозорих покриттів для скла, для покращення захисту[1].

Серед видів захисних покриттів виділяються наступні:

Віконні плівки захищають від нагрівання, та зазвичай наносяться на плоске скло з внутрішньої сторони приміщення, щоб зменшити кількість проникаючого інфрачервоного або ультрафіолетового випромінювання та видимого світла.[2] Вони є пофарбованими або металізованими, щоб перетворити сонячне випромінювання в інфрачервоне, яке потім відбивається в зовнішнє середовище. При цьому залишаючись прозорими для видимого світла.

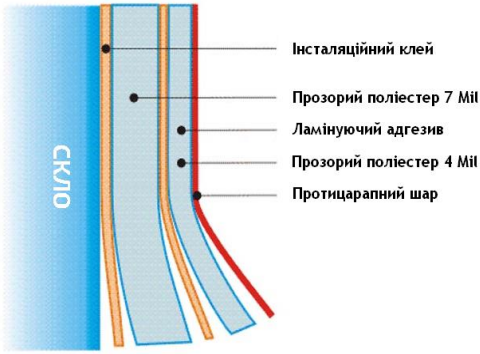
Захисні плівки наносяться для запобігання руйнування скла. Зазвичай, при використанні ці плівки виготовляються з пластика товстого перетину і призначені для забезпечення цілісності скла при сильних ударах. Ці захисні плівки часто також тонуються і можуть бути до 400 мікрон завтовшки (в 10 разів товщі, ніж звичайні тонувальні плівки).

Металізовані захисні плівки мають здатність створювати ефект однобічної видимості, вони виключають витік інформації по електромагнітному і віброакустичному каналах. Захисні плівки з металевим напиленням мають здатність знижувати інтенсивність або зовсім відфільтровувати мікрохвильове випромінювання (енергію в радіочастотному діапазоні).

Тоновані плівки забезпечують приватність, зменшуючи кількість світла, що проходить через скло. Найбільш поширений колір тонованих плівок – різні відтінки сірого, від ледь помітного затемнення до практично повного поглинання сонячного випромінювання. Вони можуть бути також дзеркальними, забезпечуючи безперешкодний вид з боку менш освітленого приміщення, але практично невидимість захищуваного приміщення з боку більш освітленого приміщення на тлі віддзеркалень. Професійно встановлені дзеркальні плівки створюють "ефект односторонньої видимості".[2]

Діелектричні інтерференційні шари. Коефіцієнт відбивання скла може бути селективно збільшений в 5-6 разів за допомогою діелектричних покриттів. Це є можливим за рахунок оптичної інтерференції, якщо достатньо великий коефіцієнт заломлення та товщина покриття кратна 1/4 і 3/4 довжини хвилі. В даному випадку мова йде про низькопоглинаючі матеріали з великим коефіцієнтом заломлення. При багатошаровому покритті з різним коефіцієнтом заломлення значно посилюється вибіркове відбивання. Світлопропускання може при цьому становитиме 80% і більше. Діелектричні покриття отримують шляхом осадження оксидованих речовин з розчинів або аерозолів. При двосторонньому покритті поверхонь скла методом занурення в розчин досягається високий ступінь однорідності і значно посилюється відбивання. Металізація методом спалювання забезпечує хорошу механічну і атмосферну стійкість.[3]

Напівпровідникові покриття. Існує цілий ряд напівпровідникових сполук, що володіють високою вибірковою відбиваючою здатністю в інфрачервоній області при хорошому світлопропусканні. Оксиди різних багатовалентних металів при використанні певних методів підготовки та осадження можуть бути нанесені на поверхню скла у вигляді мікрокристалічних шарів.



Плівка складається з декількох шарів прозорого поліестера; шару, який захищає від подряпин; інсталяційного клею (Рис.1). Інсталяційний клей являє собою стійкий до перепадів температури акриловий шар, який є самоклеючим та містить УФ поглиначі і стабілізатори.

Рисунок 1 – Структура плівки

Отже, застосування високоефективних захисних покриттів у цьому контексті стає необхідністю, щоб убезпечити важливі дані від потенційних загроз. Дослідження в галузі ефективності захисних покриттів в інформаційній безпеці технологій сприятиме подальшому розвитку і впровадженню передових розробок, забезпечуючи надійний захист наших цифрових ресурсів у сучасності

Література

1. Jones D., Kovacova A., Qiao, G. G., Polymer–Layered Silicate Nanocomposites: A Review." Polymer Reviews, 56(4), p.579-632.

2. Структура захисних плівок скла [Електронний ресурс]. – Режим доступу : http://sdi.ua/ua/types-of-films/protective-films/38-structure-of-protective-films.html

3. Pulker H.K., Coatings on Glass. Second, revised edition, 1999. 569 p.

УДК 656.7

ВИКОРИСТАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ СИСТЕМ ПРИ ВИКОНАННІ ПОШУКОВО-РЯТУВАЛЬНИХ ОПЕРАЦІЙ

Малець Богдан, Малець Ігор
Львівський національний університет ім. Івана Франка, м. Львів,
Львівський державний університет безпеки життєдіяльності, м. Львів

Цей допис описує обґрунтування ефективності застосування безпілотних повітряних суден при виконанні пошуково-рятувальних операцій та пропозиції впровадження нової технології виконання даного типу робіт.

Ключові слова: повітряне судно, пошуково-рятувальні роботи, безпілотні повітряні судна, ефективність.

This post describes the substantiation of the effectiveness of the use of unmanned aerial vehicles in the performance of search and rescue operations and offers the introduction of a new technology for the performance of this type of work.

Key words: aircraft, search and rescue operations, unmanned aircraft, efficiency.

Безпілотна авіаційна система (безпілотний авіаційна система) — безпілотне повітряне судно, пов'язані з ним пункти дистанційного пілотування (станції наземного керування), необхідні лінії керування і контролю та інші елементи, вказані в затвердженому проєкті типу цього комплексу. Цей комплекс може охоплювати декілька безпілотних літальних апаратів.

Безпілотний літальний апарат – літальний апарат, який літає та сідає без фізичної присутності пілота на його борту.

До складу БАС входять:

• БпЛА;

• пункт управління;

• система зв’язку з БпЛА (радіозв’язок або супутниковий зв’язок);

• додаткове обладнання, необхідне для перевезення та обслуговування БпЛА.

У всіх видах стихійних лих БпЛА може допомогти рятувальникам зрозуміти ситуацію та виявити постраждалих або осіб, які потребують допомоги. Це особливо актуально, коли територія важкодоступна. Такі завдання включають порятунок при лавинах, пожежах, повенях або забрудненнях, наприклад, ядерна катастрофа. У цих ситуаціях БпЛА можуть передавати не тільки візуальну інформацію, але й інші дані, такі як температура, якість повітря або радіоактивність. Крім того, БпЛА

можуть забезпечувати зв'язок для підключення до недоступних людей або навіть доставити терміново необхідні інструменти.

БпЛА мають широкі можливості для огляду великих та віддалених районів. Вони можуть передавати зображення та дані датчиків з віддалених місць швидше, ніж звичайні засоби, і без ризику нанесення шкоди людині, яка стежить за ситуацією.

Використання БАС є перспективною галуззю для виконання пошуково-рятувальних операцій і може відігравати важливу роль у їх успішному результаті. БпЛА можуть легко і швидко отримувати доступ до недоступного середовища. Вони рухливі, легко транспортуються та демонструють автономну поведінку, забезпечуючи точну та надійну підтримку в повітрі.

Завдяки вбудованим датчикам, які можуть адаптуватися до зовнішніх умов, у рятувальників є змога точно досліджувати та картографувати великі ділянки, до яких важко дістатися в режимі реального часу (важкодоступні райони, дороги, заблоковані завалами або перевантаженням транспорту), направляючи рятувальні групи до цільових місць і таким чином розширити можливості пошуку для виявлення людей, які цього потребують.

Карти розподілу ймовірностей можуть використовуватися БпЛА для проектування траєкторії польоту. Для підтримки пріоритетного пошуку БпЛА перелітає зони більшої ймовірності та забезпечує візуальну підтримку за допомогою вбудованого датчика. І навпаки, дані, зібрані БпЛА, можуть забезпечити рятувальні групи цими даними, необхідними для оновлення карт розподілу ймовірностей.

Після землетрусу або іншої катастрофи БпЛА можуть надавати інформацію про область руйнування, місцезнаходження та тяжкість пошкоджень будівлі, виявлення жертв під руїнами, надання підтримки у розробці відповідних стратегій. Землетрус на Гаїті в 2010 році став початковою точкою для експлуатації БпЛА та оцінки структурної цілісності будівель, доріг та іншої інфраструктури, яка виконується швидше та з більшою точністю. Шанс на виживання людей, що потрапили в пошкоджені будівлі, в основному залежить від видів пошкодження будівель. Отже, за допомогою швидкого картографування постраждалої території будівель можуть бути охарактеризовані та класифіковані відповідно до збитків, яких вони зазнали, у конкретному масштабі, що відповідає оцінці рятувальних груп, з метою оптимізації їх роботи.

Підхід до проведення може значно відрізнятися в залежності від сукупності зовнішніх факторів, таких як: погодні умови, час доби, місце проведення пошуково-рятувальної операції, тощо. Загалом схеми пошуку можна поділити на чотири групи, до складу якої входять: візуальний пошук, електронний пошук, пошук в темний період доби, сухопутний пошук.

Найбільш часто вживаним є візуальний пошук, який в свою чергу поділяється на: секторний пошук, пошук по квадратам, що розширюються, пошук з обстеженням лінії руху, контурний пошук.

Секторний пошук застосовується коли точно відомо місце розташування об'єкта пошуку і район пошуку невеликий. Це дозволяє в найкоротші терміни і з найбільшою імовірністю виявити постраждалих і приступити до надання допомоги. Пошук по квадратах, що розширюються найбільш ефективний в тих випадках, коли місце розташування об'єкта пошуку відомо з відносно великою точністю. Однак у порівнянні з секторним пошуком він є більш ресурсозатратним та потребує більше часу. Пошук з обстеженням лінії руху застосовується у випадку, коли повітряне або морське судно зникло без сліду при проходженні по відомому заздалегідь маршруту. Контурний пошук застосовується, якщо НС відбулася в гірській місцевості.

Варто дотримуватися надзвичайної обережності в ході здійснені пошуку в горах, каньйонах і долинах. Для такої операції використання БАС є особливо доцільним у зв'язку з високою маневреністю БпЛА та виключенням імовірності завдання шкоди екіпажу.

Коли відбуваються стихійні лиха, техногенні катастрофи, аварії на промислових підприємствах і обвалення міських інфраструктурних об'єктів, перші кілька годин мають вирішальне значення. І не тільки в цих випадках -люди можуть заблукати в лісі, горах, опинитися у відкритому морі. Якщо справа доходить до порятунку життів, ключову роль може зіграти використання передових технологій.

У 1991 році з ініціативи міжнародних команд рятувальників, які відреагували на землетрус у Вірменії в 1988 році і Мехіко в 1985 році, була заснована Міжнародна пошуково-рятувальна консультативна група (INSARAG). Ця організація ООН сприяє обміну інформацією між національними міськими пошуково-рятувальними організаціями та координації на місцях при НС.

Типи інцидентів, що вимагають пошуку і порятунку людей, в різних країнах відрізняються, оскільки ключове значення мають особливості регіону, матеріальне оснащення та теоретична підготовка фахівців. Проте, в кожному з регіонів велику роль відіграють нові і вдосконалені технології, які підвищують як безпеку самих рятувальників, так і загальну ефективність при проведенні пошуково-рятувальних операцій.

Ринок пошуково-рятувального технологій сегментується на обладнання для планування рятувальних операцій і зв'язку, пошукове, медичне і технічне обладнання. Комунікація - одна зі сфер, в якій відбулися кардинальні поліпшення. За допомогою мобільних телефонів та інших приладів можна покликати на допомогу практично з будь-якої точки планети і зорієнтуватися на місцевості.

Також існують і спеціалізовані системи: наприклад, geoDVR від RemoteGeoSystems, що дає можливість переглядати, записувати і визначати координати географічної точки і встановлювати мітку на карті. На відміну від традиційних систем відеозапису, системи geoDVR записують відео з даними про географічне місцезнаходження з прив'язкою до часу за допомогою GPS. Дані потрібні рятувальникам, щоб прийняти оптимальне рішення про те, де і як використовувати ресурси, виходячи з точного місця розташування людей і ступеня небезпеки. Завдяки можливості зіставляти і записувати інформацію і віддалено обмінюватися нею, рятувальні місії можуть стати значно ефективнішими.

DJI Airworks – міжнародна щорічна конференція, яка розвиває індустрію безпілотників. AirWorks є центром інновацій та зростання, що дозволяє учасникам цієї екосистеми обмінюватися ідеями, отримувати більше контролю над технологією БАС та керувати майбутнім розвитком галузі.

Безпілотники врятували життя як мінімум 279 людей у світі, - оголосив Ромео Дюршер, директор з інтеграції громадської безпеки DJI на AirWorks 2019. І ця цифра напевно дуже занижена, так як це лише офіційно задокументовані випадки, при цьому багато інцидентів не були зареєстровані і не згадувані в популярних світових ЗМІ. В останні роки безпілотники стали частіше застосовуватися для підтримки громадської безпеки та пошуково-рятувальних операцій. Можливо, найяскравішим прикладом цього було використання БпЛА під час і після пожежі 2019 року в соборі Нотр-Дам в Парижі.

Література

1. A. Symington, S. Waharte, S. J. Julier, and N. Trigoni, “Probabilistic target detection by camera-equipped uavs,” in ICRA, 2010.

2. Hidayatullah P., Konik H. CAMSHIFT improvement on multi-hue and multi-object tracking // Intern. Conf. on Electrical Engineering and Informatics, ICEEI 2011. Bandung, Indonesia: IEEE, 2011. P. 143—148.

3. M. Goodrich, B. Morse, D. Gerhardt, J. Cooper, M. Quigley, J. Adams, and C. Humphrey, “Supporting wilderness search and rescue using a camera-equipped mini uav: Research articles,” J. Field Robot., vol. 25, no. 1-2, pp. 89–110, 2008.

УДК 626/627.03.042.019.3

ОПИС МОДЕЛЮВАННЯ СХОДЖЕННЯ СЕЛЕВОГО ПОТОКУ ЗА РЕЛЬЄФОМ ЦИФРОВОЇ КАРТОГРАФІЧНОЇ ОСНОВИ

Мельник Максим, Рудик Юрій
Львівський державний університет безпеки життєдіяльності

Анотація. Розглядаються різновиди гідротехнічних споруд (ГТС) та конструктивних споруд. Наведені підходи для запобіганню виникнення аварій на спорудах цивільного захисту. Виходячи з подій, які нас оточують, дана тематика потребує постійної уваги та вдосконалення, задля безпеки наших співробітників та громадян України.

Ключові слова: аналіз, безпека, ГТС, аварія, надійність, сценарії, воєнний стан.

Abstract. Types of hydraulic engineering and constructive structures are considered. Approaches to prevent accidents at civil defense facilities are given. Based on the events that surround us, this topic requires constant attention and improvement, for the safety of our employees and citizens of Ukraine.

Key words: analysis, safety, hydraulic tools, accident, reliability, scenarios, martial law.

Вступ. Контроль інженерних споруд, у тому числі гідротехнічних споруд (ГТС), – це одна з головних складових підтримання їх безпеки. Заключна стадія контролю гідротехнічних споруд (ГТС) складається з винесення оцінок фактичного стану споруд і рівня надійності їх експлуатації та безпеки. На основі цих оцінок вибудовується комплекс заходів для підтримки такого рівня надійності і безпеки споруд, що відповідає нормативним і проектним вимогам [1].

Проаналізовано параметри безпеки для оцінювання таких різновидів ГТС, як греблі та дамби. Дамба - гідротехнічна споруда періодичної дії з огороджувальною ознакою. Одним з основних призначень греблі є підняття рівня води у річці на певну висоту і регулювання цього рівня, що досягається будівництвом водопідпірної греблі. Зокрема, можна зробити висновок про призначення гідровузла, в який входить гребля, і про склад інших споруд, які складають цей гідровузол [2]. Цікавим в цьому плані є приклад щодо забезпечення безпеки Кам'янської дамби довжиною 8,2 км та Знам'янської дамби обвалування довжиною 7,2 км, побудованих за проектом Укргідропроекту для захисту земель та населених пунктів площею 16 тис. га на території «Кам'янського поду» у Запорізькій області. Різниця позначок води у Каховському водосховищі та позначок території, що захищається, на зазначеній ділянці становить від 12 м та 8 м [3]. Горизонтальна складова тиску води на греблю зростає з глибиною, будучи рівною добутку Wh, де h- глибина і W-вага одиниці об'єму води. Отже, сумарний гідростатичний тиск на одиничну довжину елементу поперечного перерізу полотна греблі складає 1/2 (Wh2).

Проблеми запобігання аваріям на греблях та дамбах повинні вирішуватись при реалізації комплексних попереджувальних та захисно-профілактичних заходів [2]. Заходи протидії небезпекам гідродинамічного характеру. Основними вражаючими факторами катастрофічного затоплення є руйнівна хвиля прориву та водяний потік. Гідродинамічна аварія – це надзвичайна подія, пов'язана з виходом із ладу гідротехнічної споруди чи її частини та некерованим переміщенням великих мас води, які несуть руйнування і затоплення великих територій. Важливу роль у забезпеченні надійної роботи об’єднаної енергетичної системи України, в умовах воєнного стану, відіграють гідровузли Дніпровського каскаду гідроелектростанцій [4].

Прорив греблі – це початкова фаза гідродинамічної аварії і являє собою процес утворення прорану і некерованого потоку води з водоймища верхнього б'єфа, що спрямовується через проран у нижній б'єф. Хвиля прориву утворюється у фронті потоку води, що спрямовується в проран і має, як правило, значну висоту гребеня, швидкість руху і велику руйнівну силу. Швидкість просування води прориву коливається в межах від 3 до 25 км/год. В результаті великих гідродинамічних аварій гинуть люди, переривається подача електроенергії в енергетичні системи, припиняється функціонування водогосподарських систем, руйнуються чи опиняються під водою населені пункти і промислові підприємства, виводяться з ладу комунікації й інші елементи інфраструктури, порушується життєдіяльність населення і виробничо-економічна діяльність підприємств, наносяться великі збитки природному середовищу, в тому числі в результаті змін ландшафту [5].

На території нашої держави побудована значна кількість критично важливих об’єктів. Одним з них є Дніпровський гідро-технічний комплекс, який щільно пов’язаний з інформаційними, енергетичними і транспортними мережами [7]. Виходячи з теперішнього розвитку сучасних технологій, в умовах повномаштабної війни, важливим аспектом безпеки об’єктів критичної інфраструктури є захист від кібератак. Додаткову інформацію ми можемо використати з указу президента США № 13010 «Про роботу по дослідженню вразливості захисту критичної інфраструктури від кібернетичних і фізичних загроз» [6].

Як не дивно сьогоднішній світ постійно прогресує, а з ним і наявні засоби та технології. Методики оцінювання стану критичної інфраструктури, а саме ГТС, не виняток у цьому плані. Поширені способи перевірки даних захисних споруд шляхом оцінки справності кожного окремого компоненту стають неефективними. Пропонується внести до розгляду нові системи аналізу, які складаються з одного або кількох пасивних та/або активних датчиків, здатних отримувати щільні та точні дані. Для цього варто покласти в майбутньому виявлення пошкодження ГТС на аналіз цифрових зображень і дані LiDAR (Виявлення оптичних параметрів та визначення дальності). Дані LiDAR дають результати, які, безсумнівно, є більш точними, ніж отримані за допомогою традиційних методів. Крім того, технологія LiDAR з роками вдосконалилася, що призвело до більшої ефективності,

швидкості та продуктивності. Техніка лазерного сканування (ЛС) дозволяє отримати точні профілі і дозволяє аналізувати всю споруду, а не окремі її частини, як це часто робить традиційний аналіз. Технологія мобільного лазерного сканера (МЛС) наразі є одним із перспективних напрямків у галузі дистанційного зондування. Оцінка стану ГТС, зроблена на основі даних МЛС, в майбутньому повинна стати однією з головних напрямів впровадження та досліджень фахівцями цивільної безпеки України, враховуючи високу швидкість збору даних та ефективність техніки.

З огляду на теперішні умови, нормативне обґрунтування та термінологія стосовно контролю захисних споруд цивільного захисту, а саме гідротехнічних, та оцінок щодо їх справності потребує комплексу заходів стосовно впорядкування, узгодження та вдосконалення. Особливо важливим напрямком є врахування умов воєнного стану та ведення інтенсивних бойових дій з застосуванням великої кількості обстрілів, що суттєво впливає на подальше проектування та планування заходів, які спрямовані на подальшу експлуатацію ГТС. Це важливо, особливо з огляду на те, що створюється небезпека загрози життю та здоров'ю працівникам ДСНС під час проведення розрахунків на цих захисних спорудах. Для оцінки безпеки кількох ГТС, які знаходяться поруч, слід у комплексі оцінювати всі складові водопідпірних засобів які приймають на себе натиск напірного фронту, а також усі елементи гідромеханічного обладнання, що тримають напір [5].

Література

1. Білик С.І., Петровськитй В.Л., Рудик Ю. І. Адаптація систем оцінювання за показниками безпеки в умовах особливого періоду Охорона праці: освіта і практика. Зб. наук. праць ІІІ Всеукраїнської науково–практичної конференції викладачів та фахівців–практиків, Львів, 2023. С.50-54.

2. Захист населення і територій від надзвичайних ситуацій. Т. 3. Інженернотехнічні заходи цивільного захисту (цивільної оборони) та містобудування. / За загальною редакцією В.В. Могильниченка. – К.: КІМ, 2008.-152 с.

3. ДБН В.1.1-24:2009 Захист від небезпечних геологічних процесів, шкідливих експлуатаційних впливів, пожежі.

4. Мозговий А. О. Імовірнісна оцінка надійності і безпеки ГТС каскадів гідроелектростнанцій. - 2019.

5. Шульга В.А. Вдосконалений алгоритм діагностичного контролю ГТС. - 2017.

6. PDD-63, May, 1998: Critical Infrastructure Protection [Електронний ресурс]. Federation of American Scientists. – Режим доступу: http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf.

7. В.М. Чернета. Моделювання загроз та управління ризиками надзвичайних ситуацій на об’єктах критичної інфраструктури України. 2021.

УДК 004.413

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В УПРАВЛІННЯ ІТ ПРОЄКТАМИ

Мечус Христина, Кордунова Юлія, Смотр Ольга
Львівський державний університет безпеки життєдіяльності, м. Львів

Робота присвячена дослідженню сучасних інформаційних технологій управління ІТ проєктами, в розрізі їх можливостей, ефективності, сегменту застосування тощо. На підставі проведеного дослідження зроблені рекомендації щодо доцільності використання тих чи інших інформаційних технологій управління ІТ проєктами в залежності від типу проєкту, методології його розробки, часових та фінансових обмежень проєкту

Ключові слова: ІТ-проєкт, інформаційні технології, Agile методології, .

The work is dedicated to the exploration of modern information technologies in IT project management, considering their capabilities, effectiveness, application segments, etc. Based on the conducted research, recommendations are provided regarding the feasibility of using specific information technologies in IT project management, depending on the project type, development methodology, and project's time and financial constraints.

Keywords: IT project, information technologies, Agile methodologies**.**

Навіть у непростих умовах сучасності, ІТ-галузь продемонструвала високий рівень адаптації до умов війни і підтримує фінансову стабільність. У сфері реалізації ІТ-проєктів використовуються різні інструменти розробки та методології управління. Вибір методології впливає на якість та ефективність реалізації проєктів, що робить важливим управління роботою команди. Сучасні проєкти характеризуються високою складністю, постійними змінами у термінах та ресурсах, що призвело до розробки та впровадження сучасних інформаційних технологій для ефективного управління проєктами. Використання інформаційних технологій управління є ключовим для вирішення цих проблем.

Мета даної роботи - проаналізувати існуючі інформаційні технології в управлінні проєктами та детально розглянути провідні інформаційні системи управління проєктами, зокрема у контексті ІТ-проєктів.

На сьогодні існує багато тлумачень поняття "проєкт". Одне з найпопулярніших: "Проєкт - це комплекс конкретних дій, спрямованих на досягнення визначених цілей протягом обмеженого часу за обмежених ресурсів". Управління проєктами, часто визначене як мова спілкування між учасниками проєкту, включає в себе методологію, яка представляє собою набір принципів та процедур для ефективного управління проєктом. У ІТ-галузі для керування проєктами все більше використовують інформаційні технології. Інформаційні системи управління проєктами підвищують ефективність управління, зменшуючи кількість невиконаних завдань і дозволяючи комплексно керувати проєктом.

Інформаційні технології допомагають поліпшити комунікацію між учасниками проєкту, виявляти та реагувати на відхилення від плану, ефективно документувати всі етапи проєкту та забезпечувати оперативний контроль. У сфері управління IT-проєктами використовуються різні інформаційні системи, включаючи "Microsoft Office Project", яка розроблена для управління проєктами будь-якої складності та включає різні рівні продуктів, спрямованих на різні потреби користувачів; «Jira» розроблена для управління агільними проєктами, вона дозволяє створювати та відстежувати задачі, управляти релізами та планувати спринти; Asana надає інструменти для планування та відстеження завдань, комунікації у команді, а також аналізу прогресу проєкту. Ці інформаційні технології дозволяють підвищити ефективність управління IT-проєктами, спрощуючи процеси планування, відстеження та звітності. Важливо враховувати конкретні потреби та характеристики проєкту під час вибору інструменту або системи для керування проєктом.

«Primavera Inc» пропонує кілька продуктів для управління проєктами: «SureTrak Project Manager», призначений для управління проєктами на нижчих рівнях складності; «Primavera Project Planner», професійний пакет для роботи зі складними багатозадачними проєктами; та «Primavera Project Planner for the Enterprise», який є основним продуктом в складі «Primavera Enterprise». Останній забезпечує планування, бюджетування, аналіз та координацію робіт, дозволяючи отримати загальну картину за конкретним проєктом чи декількома, виконати укрупнений аналіз за категоріями та статтями витрат, а також контролювати терміни та фактичні результати.

«Open Plan» використовується на всіх рівнях контролю та управління проєктами. Цей продукт допомагає створювати плани проєктів, враховуючи обмеження, визначає рівні пріоритетності проєктів, задає важливість проєктів для розподілу ресурсів, мінімізує ризики та проводить детальний аналіз робіт.

Таким чином, вибір інформаційної системи для управління проєктами визначається необхідністю управління конкретними проєктами. Перед впровадженням технологій управління IT-проєктами важливо визначити, які саме проєкти потребують управління. Ефективність системи управління визначається витратами та прибутками, які вона спричинить. Перед початком використання інформаційних технологій управління IT-проєктами, необхідно скласти детальний план впровадження, виконати ресурсне планування та впровадити контроль витрат на проєкт, щоб уникнути негативних наслідків та стресу серед співробітників.

Сучасні інформаційні технології в управлінні IT-проектами виявляють значний вплив на ефективність та успішність виконання проектів. Вони надають широкий спектр інструментів для планування, відстеження прогресу, комунікації та співпраці, що дозволяє командам краще керувати ресурсами та виконувати завдання вчасно та ефективно.

Застосування сучасних систем управління проектами, таких як Jira, Asana, Trello, дозволяє створювати структуровані плани, контролювати виконання завдань та пристосовуватись до змін у процесі роботи. Agile методології розробки програмного забезпечення, зокрема такі, як Scrum, Kanban надають гнучкість та можливість швидко реагувати на вимоги ринку, поліпшуючи продуктивність розробки.

Використання віртуальних та хмарних технологій сприяє зручній спільній роботі команд, навіть у віддалених режимах роботи. Автоматизація процесів через DevOps інструменти допомагає автоматизувати рутинні завдання та забезпечує безперервну поставку програмного забезпечення.

Інноваційні технології управління ІТ-проектами, сприяють підвищенню продуктивності, зниженню ризиків та досягненню успішних результатів у виконанні проектів. Застосування цих інноваційних технологій в управлінні ІТ-проектами дозволяє покращити спроможність аналізувати дані та робити швидкі та обґрунтовані рішення на основі цих даних. Вони забезпечують високу ступінь прозорості і контролю над процесами, що дає можливість оперативно реагувати на зміни та використовувати ці зміни як можливості для вдосконалення проекту.

Додатково, сучасні технології управління ІТ-проектами сприяють покращенню комунікації, як всередині команди так і з стейкхолдерами, що у свою чергу сприяє збільшенню їх залученості до процесу та зниженню ризиків, пов'язаних з непорозуміннями, своєчасною непоінформованістю, неузгодженістю дій тощо.

Загалом, сучасні інформаційні технології управління ІТ-проектами стають критично необхідними для досягнення успіху в сфері управління ІТ-проєктами, дозволяючи оптимізувати процеси, забезпечувати якість продукту та здійснювати ефективне управління ресурсами.

Література

1. Kerzner, H. (2017). Project Management: A Systems Approach to Planning, Scheduling, and Controlling. Wiley.

2. Schwalbe, K. (2020). Information Technology Project Management. Cengage Learning.

3. Кордунова Ю. С., Смотр О. О., Кокотко І. Я., Малець Р. Б. Аналіз традиційного та гнучкого підходів до створення програмного забезпечення в динамічних умовах. Управління розвитком складних систем. Київ, 2021. № 47. С. 71 – 77, https://doi.org/10.32347/2412-9933.2021.47.71-77

4. Kordunova, Y., Prydatko, O., Smotr, O., Golovatyi, R. (2023). Expert Decision Support System Modeling in Lifecycle Management of Specialized Software. In: Babichev, S., Lytvynenko, V. (eds) Lecture Notes in Data Engineering, Computational Intelligence, and Decision Making. ISDMCI 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 149, pp 367–383. Springer, Cham. https://doi.org/10.1007/978-3-031-16203-9_22

УДК 004.42

АВТОМАТИЗАЦІЯ ПРОЦЕСУ КОМУНІКАЦІЇ ТА ІНФОРМУВАННЯ СТУДЕНТІВ В НАВЧАЛЬНОМУ ЗАКЛАДІ ЗАСОБАМИ TELEGRAM БОТУ

Мигасюк Роман, Смотр Ольга, Придатко Олександр
Львівський державний університет безпеки життєдіяльності, м. Львів

Робота присвячена розробці Telegram Боту для автоматизації процесу комунікації та інформування студентів навчального закладу, щодо університетських новин, розкладу тощо. Розроблено та реалізовано проект на основі мови програмування Python з використанням бібліотеки aiogram, бази даних Postgresql та Rest API за допомогою фреймворка Django.

Ключові слова: чат-бот, Telegram, Python, Django, DRF

This work is devoted to the development of Telegram bot that aims to automate the process of communication and informing students of the educational institution about university news, schedules, etc. The project is created using Python programming language, aiogram library, Postgresql database and Rest API by Django framework.

Key words: Bot, Python, DBMS, Telegram, Django, DRF.

Чат-бот (англ. Chatbot) − комп'ютерна програма, розроблена на основі нейромереж та технологій машинного навчання, за допомогою якої можливо здійснювати комунікацію в аудіо- або текстовому форматі. Чат-бот використовують для виконання конкретних завдань (наприклад, отримання довідкової інформації, виконання розрахунків) або задля розваги. Він створюється людиною для людей та навчається під певне коло цілей. Чат-бот імітує розмову з людиною в Інтернеті, саме тому даний сервіс найкраще зарекомендував себе в месенджерах. Месенджери це програми для обміну повідомленнями в реальному часі через інтернет. Найпопулярнішими месенджерами в Україні є Viber, Telegram, Facebook Messenger, WhatsApp. З кожним роком тенденція використання чат-ботів у сфері надання послуг(замовлення їжі, товару, запис до перукаря, тощо), зростає.

Виникає питання, чому не використовувати чат-ботів у навчальному процесі. Хоча б, для прикладу, для автоматизації сервісу отримання розкладу занять в навчальному закладі, розсилки новин закладу тощо. Звісно ж у нашому університеті є сайт з електронним розкладом, працює правильно, але не «запам'ятовує» ні курс, ні групу. Отож, щоразу необхідно заходити в браузер, шукати сайт, вводити групу, дату, тобто займатися монотонною роботою та витрачати час. Тому було прийнято рішення розробити чат-бот, що допоможе вирішити ці проблеми та надасть можливість реалізувати, ще ряд корисних послуг, для прикладу, надсилання щоденного розкладу, можливість для викладача надіслати повідомлення студентам обраних груп. Розроблятимемо Telegram бот.

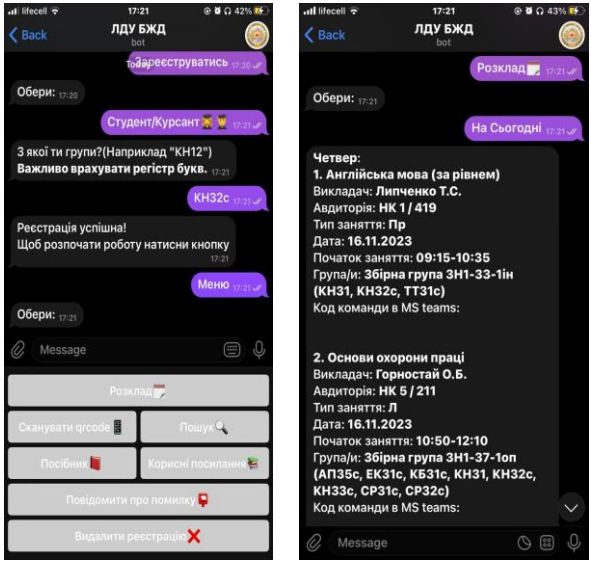
Чому Телеграм? Telegram – останнім часом зарекомендував себе як один з месенджерів з найбільш швидко зростаючою аудиторією, Адже, більшість студентів мають свої бесіди груп саме у Telegram, тому можливість адаптації Бота під чат є перспективною та цікавою. Окрім цього, Telegram API надає користувачу великий спектр можливостей у реалізації чат-бота, а саме:

- Багатомовність, у написанні чат-ботів, можна використовувати такі мови як: Python; Java; JS та багато інших.
- Сервіси конструктори Ботів та сервіси з готовими шаблонами.
- Кросплатформність, Телеграм реалізований на IOS, Android як мобільний додаток та десктопні ОС Windows, MacOS, Linux, також є веб-версія застосунку.

Для написання чат-боту ми вирішили використовувати Python, зважаючи на великий вибір бібліотек для написання, простоту та структурованість коду. Та обрали саме aiogram бібліотеку.

Чому aiogram?

- Асинхронність – процес обробки введення\виведення, що дозволяє продовжити обробку інших завдань, не чекаючи завершення попереднього завдання.
- Підтримка розробників, часті оновлення, бібліотека не стоїть на місці, а постійно розвивається, додаються нові можливості для розробки.



а) б)

Рисунок 1 – Скрін екрану роботи Telegram –бота «ЛДУ БЖД»
а) Процес реєстрації; б) Процес отримання розкладу

Вибір використання фреймворку Django був здійснений з метою ефективної розробки та управління бекенд-складовою проекту. Django, надає готові інструменти для швидкого створення високопродуктивних веб-додатків. Його інтегровані можливості, такі як аутентифікація користувачів, обробка форм, адміністративний панель, та вбудована підтримка ORM для взаємодії з базою даних, роблять Django потужним інструментом для розробки великих та складних проектів. Крім того, Django REST Framework надає зручний спосіб побудови API для взаємодії з чат-ботом, що сприяє високій швидкості розробки та надійності системи.

Підсумовуючи вищенаведене, можна стверджувати, що на сьогодні, розробка власного чат-бота є актуальною, цікавою та технічно здійсненною задачею. Вибір Telegram месенджера та мови програмування Python, для розробки чат бота є обґрунтованими.

Література

1. Чат-бот. [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A7%D0%B0%D1%82-%D0%B1%D0%BE%D1%82

2. Топ-10 популярних месенджерів світу та України у 2023 році. [Електронний ресурс]. – Режим доступу: https://sitecat.net/review/top-10-popular-messengers/

3. Українські IT-експерти назвали найбезпечніші месенджери 2022 року. [Електронний ресурс]. – Режим доступу: https://hmarochos.kiev.ua/2022/04/12/ukrayinski-it-eksperty-nazvaly-najbezpechnishi-mesendzhery/

4. Офіційний сайт Telegram. Електронний ресурс Telegram API. URL:https://core.telegram.org/api

5. Офіційна документація Django: https://docs.djangoproject.com/en/4.2/

УДК 004.451.4

ОПЕРАЦІЙНІ СИСТЕМИ ТА СИСТЕМНЕ ПРОГРАМУВАННЯ В ОРГАНАХ ТА ПІДРОЗДІЛАХ ЦИВІЛЬНОГО ЗАХИСТУ

Мисько Роман, Райта Діана
Львівський державний університет безпеки життєдіяльності, м. Львів

Дана робота досліджує важливість та роль операційних систем і системного програмування у сфері цивільного захисту. Зосереджуючись на їхньому впливі на ефективність управління різноманітними процесами та реагування на надзвичайні ситуації, робота аналізує використання різноманітних операційних систем та програмного забезпечення для координації дій, аналізу даних та оперативного реагування на кризові ситуації. Висвітлюючи інтеграцію спеціалізованих систем управління та аналізу, автор підкреслює їхню роль у оперативному отриманні необхідної інформації та прийнятті обґрунтованих рішень. Робота також розглядає важливість системного програмування для створення спеціалізованих програм та алгоритмів, що автоматизують управління, прогнозування подій та моделювання сценаріїв для підвищення ефективності реагування на небезпеку. Враховуючи потреби сфери цивільного захисту, робота акцентує на важливості розвитку технологій у цих галузях для забезпечення максимальної безпеки громадян та інфраструктури у надзвичайних ситуаціях.

Ключові слова: операційні системи, системне програмування, цивільний захист.

This paper explores the importance and role of operating systems and system programming in the field of civil protection. Focusing on their impact on the efficiency of managing various processes and responding to emergencies, the paper analyzes the use of various operating systems and software for coordinating actions, data analysis, and prompt response to crisis situations. Highlighting the integration of specialized management and analysis systems, the author emphasizes their role in promptly obtaining necessary information and making informed decisions. The paper also examines the significance of system programming in creating specialized programs and algorithms that automate management, event forecasting, and scenario modeling to enhance responsiveness to hazards. Considering the needs of the civil protection sector, the paper underscores the importance of technological advancement in these areas to ensure maximum safety for citizens and infrastructure during emergencies.

***Keywords*:** operating systems, system programming.

Операційні системи та системне програмування мають важливе значення в сфері цивільного захисту, забезпечуючи ефективне управління різноманітними процесами та системами, які забезпечують безпеку та реагують на надзвичайні ситуації. Органи та підрозділи цивільного захисту використовують різні операційні системи та програмне забезпечення для координації дій, аналізу даних та швидкого реагування на кризові ситуації.

Інтеграція спеціалізованих операційних систем у роботу з електронними картами, системами моніторингу, аналізу великих обсягів даних та зв'язку дозволяє оперативно отримувати необхідну інформацію та приймати обґрунтовані рішення в умовах надзвичайних ситуацій. Крім того, системне програмування дозволяє створювати спеціалізовані програми та алгоритми для автоматизації процесів управління, прогнозування подій та моделювання сценаріїв, що сприяє підвищенню ефективності реагування на небезпеку.

Завдяки розвитку технологій операційних систем та програмного забезпечення, органи цивільного захисту отримують можливість не лише ефективно керувати ситуацією під час надзвичайних подій, але й аналізувати минулі події для покращення стратегій та планів дій у майбутньому.

Зважаючи на значення та важливість цивільного захисту, розробка спеціалізованих операційних систем та програмного забезпечення відповідає потребам в управлінні кризовими ситуаціями. Ці системи включають в себе елементи телекомунікаційного зв'язку для швидкої передачі даних та командних інструкцій, модулі управління ресурсами та координації дій рятувальних підрозділів.

Застосування системного програмування також дозволяє створювати аналітичні інструменти для прогнозування ризиків та визначення оптимальних шляхів реагування в реальному часі. Це сприяє не лише оперативній реакції на небезпеку, але й підвищує рівень попередження та готовності до можливих загроз.

Поміж ключових аспектів можливо відзначити вдосконалення систем моніторингу за допомогою дронів та супутникового спостереження, розробку спеціалізованих програм для швидкого аналізу та обробки великих обсягів даних, а також розробку інтерфейсів, які забезпечують швидку інтеграцію різних систем та джерел інформації.

Це спрямовано не лише на вдосконалення реакції у випадку кризових ситуацій, а й на підвищення ефективності, координації та спільної діяльності рятувальних служб для забезпечення максимальної безпеки громадян та інфраструктури в умовах надзвичайних подій.

Література

1. Зачко О.Б., Головатий О.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. Khlevnoi, O.: Standardization of fire safety requirements for evacuation routes and exits in secondary education institutions with inclusive education. Ph.D. thesis, Lviv State University of Life Safety (2021)

3. Борзов Ю. Особливості застосування комп‘ютерного моделювання для покращення навчального процесу / Ю. Борзов, Р. Головатий, Я. Магеровський. // Інформаційні технології розвитку змісту освіти. – 2019. – С. 80–81.

УДК 004.9

РОЗРОБКА СЦЕНАРІЇВ РОЗВИТКУ ПОДІЙ З ВИКОРИСТАННЯМ LARGE LANGUAGE MODEL

Нечипорук Вікторія
Київський національний університет імені Тараса Шевченка

Анотація. Аналізуючи можливості використання LLM для генерації сценаріїв та стратегій, робиться акцент на розробці шаблонів запитів для отримання сталих результатів. Розглядається важливість впровадження точних термінів і вказівок для кращої взаємодії з моделлю та забезпечення різноманітних відповідей.

Ключові слова : Large Language Model, сценарний аналіз, ChatGPT, запити, семантичні ролі.

Abstract. Analyzing the potential use of LLM for generating scenarios and strategies, emphasis is placed on developing query templates to achieve consistent outcomes. The importance of implementing precise terms and instructions for better model interaction and ensuring diverse responses is being considered.

Keywords : Large Language Model, scenario analysis, ChatGPT, prompts, semantic roles.

Поява Large Language Model (моделей глибокого навчання, призначених для обробки та розуміння великих обсягів даних на природній мові), таких як чат GPT, сприяє кращому вирішенню широкого спектру задач.

Однією з таких важливих задач є генерація сценаріїв майбутнього, стратегій, плану розгортання подальших подій, попередньо описавши певні обставини та факти. Проблематика цього питання полягає в складності правильного написання дієвих запитів до великої мовної моделі, що даватимуть бажаний результат, адже LLM – це свого роду нова парадигма програмування, яка формується людською мовою. Для вирішення якоїсь задачі потрібно створити спеціальну мову запитів, щоб не втратити контекст і увагу на основі машинного навчання. Саме це і є розробка шаблонів запитів, щоб отримати сталі відповіді на питання.

Дана задача є актуальною, так як створення інструментів для генерації основи сценаріїв може бути корисна у багатьох напрямках, таких як прогнозування результатів та наслідків при моделюванні різних можливих варіантів подій, планування стратегій відповідно до різних можливих сценаріїв, ризик – менеджмент та підтримка прийняття рішень. Також актуальність цього дослідження визначається необхідністю автоматизувати аспекти сценарного аналізу, зважаючи на активне впровадження технологій штучного інтелекту (LLM) в аналізі та узагальненні інформації. У результаті можна створити інструмент для використання у супроводженні проце-

су створення сценаріїв, який базується на послідовному застосуванні шаблонів запиті до великої мовної моделі. Керуючи увагою LLM, ці запити допомагають отримати стало відформатовані компоненти сценаріїв у відповідь на поставлені користувачем завдання. Механізми уваги в LLM, зокрема механізм self-attention, що використовується в трансформерах, дозволяють моделі зважувати важливість різних слів або фраз у певному контексті. Призначаючи різну вагу токенам у вхідній послідовності, модель може зосередитися на найбільш релевантній інформації, ігноруючи менш важливі деталі. Ця здатність вибірково фокусуватися на певних частинах вхідних даних має вирішальне значення для виявлення довгострокових залежностей і розуміння нюансів природної мови.

Для побудови сценаріїв використовується відома методологія сценарного аналізу на основі дослідження та аналізу потенційних тенденцій і впливових факторів. Структура для написання потрібних сценаріїв майбутнього складається з наступних пунктів : визначення цілей, вибір ключових факторів, аналіз впливу факторів, створення сценаріїв, оцінка сценаріїв, вибір стратегії, моніторинг та корекція. Цей метод можна використовувати, задавши дану структуру як питання до LLM, наприклад : «Мені потрібно написати сценарії майбутнього використовуючи сценарний аналіз».

Наступним кроком потрібно в запиті коротко описати хвилюючу проблему та попросити ChatGPT надати основні ключові технології у розв'язанні цього питання. Далі, отримавши потрібну відповідь, можна зробити запит на оптимістичний, проміжний, песимістичний сценаріїв на задану кількість кроків, а також стратегії та їх моніторинг як наслідок з попереднього. Як приклад, можна взяти коронавірус, коротко описавши симптоми хвороби, інтенсивність та локалізацію спалаху вірусу, але чітко не вказуючи, що це саме коронавірус, а вказати як невідому нову хворобу. У результаті, можна отримати ключові технології боротьби з новим невідомим вірусом, сценарії поширення хвороби, стратегії і моніторинг даної нової епідемії.

Використовуючи так звані prompts або шаблони запитів, тобто інструкції для LLM, виконується дотримання правил, автоматизація процесів і забезпечення якостей згенерованих результатів. Таким чином можна спрямовано впливати на згенеровані відповіді шляхом подання конкретних запитань, уточнень або вказівок. Це дозволяє точніше керувати напрямком розмови та отримувати більш узгоджені відповіді, підкреслюючи специфічні потреби чи завдання.

Для того, щоб зробити правильні запити, застосовуються спеціальні лінгвістичні терміни, які задають семантично для однозначного виводу результатів. Дуже важливо працювати з моделлю, не втративши механізм уваги моделі. Це вдасться зробити завдяки шаблонним запитам та прямого вказання семантичних ролей. Оскільки, якщо запитати модель напряму, сталих результатів не буде, але якщо запитувати як лінгвісти, то отримуються потрібні

відповіді. При цьому зміщується механізм самоуваги моделі, але не втрачається контекст, так як модель керується лінгвістичними запитами і семантичними ролями. До прикладу можна взяти семантичну роль «суперечник», тобто особа (предмет), що перешкоджає виконанню дії. Відповідно можна створити запит : «Надай мені перелік об'єктів за семантичною роллю «Суперечник» («Стимул») до сценарію «Оптимістичний («Проміжний», «Песимістичний») сценарій», внаслідок чого будуть формуватися перешкоди та сприяючі фактори сформованих картин майбутнього.

Таким чином, впроваджуючи Large Language Models, можна краще розуміти та генерувати складні сценарії майбутнього, а також розробляти стратегії відповідно до різних умов. Це можливо завдяки створенню шаблонів запитів, які дозволяють отримувати сталі та узгоджені відповіді. Такий підхід допомагає точніше керувати розмовою та забезпечує якісний вихідний результат. При цьому важливо враховувати механізми уваги в моделі, використовуючи лінгвістичні терміни та семантичні ролі для забезпечення правильного контексту в запитах.

Література

1. Jungwirth D., Haluza D., AI-Based Scenario Generation for Future Planning: An Exploratory Study Using GPT URL: https://www.opastpublishers.com/open-access-articles/aibased-scenario-generation-for-future-planningan exploratory-study-using-gpt3.pdf (Last accessed: 10.04.2023).

2. Нечипорук, В. О. Створення сценаріїв розвитку системи на базі LLM : дипломна робота бакалавра : 124 Системний аналіз / Нечипорук Вікторія Олександрівна. – Київ, 2023. – 93 с. URL : https://ela.kpi.ua/handle/123456789/60506 .

3. Загірська І.О., Бідюк П.І. Методика побудови сценарного аналізу із використанням байєсівських методів. Електротехнічні та комп’ютерні системи. 2012. №8. С. 137–142.

4. White, Jules & Fu, Quchen & Hays, Sam & Sandborn, Michael & Olea, Carlos & Gilbert, Henry & Elnashar, Ashraf & Spencer-Smith, Jesse & Schmidt, Douglas. A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT. 2023. URL: https://arxiv.org/pdf/2302.11382.pdf (Last accessed: 15.04.2023).

УДК 721:004.8

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В АРХІТЕКТУРІ

Нєгов Марк, Гумен Олена, Селіна Ірина
Національний технічний університет України,
"Київський політехнічний інститут імені Ігоря Сікорського", Київ

Анотація. З розвитком технологій розширюється і обсяг, в якому може працювати штучний інтелект. У наш час в архітектурі штучний інтелект використовується для моделювання будівель, приміщень та інших архітектурних конструкцій. Наведено приклад використання штучного інтелекту в архітектурі при моделюванні об'єктів, а також новий стиль, вигаданий штучним інтелектом.

Ключові слова. Штучний інтелект, архітектура, моделювання, технологія BIM.

Abstract. With the development of technologies the scope in which artificial intelligence can work also expands. Nowadays, in architecture, artificial intelligence is used to model buildings, premises and other architectural structures. An example of the use of artificial intelligence in architecture when modeling objects is given, as well as a new style invented by artificial intelligence.

Keywords. Artificial intelligence, architecture, modeling, BIM technology.

Штучний інтелект швидко розвивається кожного дня і його використання у такій важливій сфері нашого життя як архітектура стає все помітнішим. ШІ може писати вірші, наукові роботи і навіть програмний код. З розвитком технологій, розширюється і обсяг, в якому може працювати штучний інтелект, тож люди почали використовувати його всюди, у тому числі і архітектурі. Штучний інтелект – це метод змусити комп'ютер чи програмне забезпечення «мислити» як людський мозок. Це досягається шляхом вивчення закономірностей роботи людського мозку та аналізу когнітивних процесів. Результатом цих досліджень є розробка інтелектуального програмного забезпечення та систем.

Так, шеньчженська архітекторка Ваньюй Хе заснувала стартап XKool, що може спроєктувати і сконструювати з нуля готовий проект готельного комплексу на 500 номерів – з усіма інтер'єрами, планами комунікацій, схемами – за лічені хвилини [1]. Дизайнер Тім Фу використав LookX для перетворення зім'ятого папірця на макет будівлі у стилі SANAA (рис.1). Подібний готель вже було спроєктовано і збудовано у Шеньчжені живими людьми, але в них ця робота зайняла чотири з половиною місяці (рис.2).

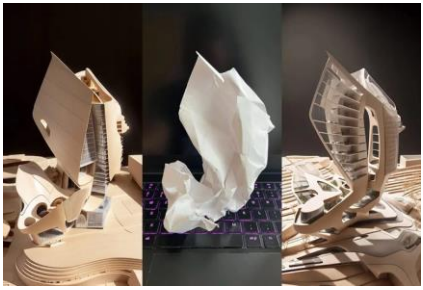


Рисунок 1 – Дизайнерська робота (Тім Фу)

Рисунок 2 – Готель, спроєктований XKool

Інструменти 3D-моделювання та ШІ співіснують у тісному взаємозв'язку. Вже розроблені програми, що дозволяють користувачам відтворювати моделі з кількох простих зображень, а перетворення тексту в 3D поступово стає реальністю завдяки публікаціям науковців, які досліджують цю тему та розвивають можливість її використання на практиці. В архітектурі, інженерії та будівництві ми вже бачимо, як деякі компанії запускають додатки на кшталт text-to-BIM, що дозволяють користувачам створювати детальні моделі будівель, використовуючи текстові підказки та спеціалізовані інструменти BIM і CAD [2].

Технологія BIM, технологія інформаційного моделювання, вже давно використовується архітекторами – будівлі, спроєктовані за допомогою цієї технології, пройшли всі перевірки і досі стоять не зруйновані. Оскільки технології на даний момент розвиваються дуже швидко, скоро процес конструювання, тестування і проєктування буде повністю автоматизований: ввід характеристик будівлі і її тип у штучний інтелект – буде достатньою інформацією для її повної побудови на папері. Професія архітекторів вже втрачає робочі місця через штучний інтелект, але в майбутньому ця галузь роботи може повністю зникнути з біржі праці [3].

ШІ не тільки може повністю замінити людину при виконанні завдань у архітектурі, а ще й перевершити людину за багатьма показниками. Китайский архітектор Тім Фу зазначив, що штучний інтелект може покласти початок новій епосі архітектури і будівництва – "неокласичному футуризму". Цей жанр заснований на поєднанні двох абсолютно різних стилів архітектури у щось нове та незвичайне.

"Найкраща здатність ШІ – поєднувати речі. Якщо ви візьмете дві різні концепції, які є дуже впізнаваними, і змішаєте їх, цей гібридний підхід дасть вам дуже успішний і унікальний результат, до того ж новий", – каже архітектор [4].

Рисунок 3 – Приклади неокласичного футуризму, виконані суто ШІ

Отже, штучний інтелект – це революційна технологія, що в багатьох галузях ВЖЕ може повністю замінити людський фактор, у тому числі і в галузі архітектури. Штучний інтелект в архітектурі створює високоякісні моделі будівель, що відповідають усім умовам і правилам проєктування.

Література

1. Хмарочос – Штучний інтелект вже значно перевершує можливості архітекторів– https://hmarochos.kiev.ua/2023/08/09/shtuchnyj-intelekt-vzhe-znachno-perevershuye-mozhlyvosti-arhitektoriv-yak-programy-dopomagayut-proyektuvalnykam-i-chy-vidberut-u-nyh-robotu.

2. Дніпровське Інвестиційне Агентство – Наскільки штучний інтелект може бути корисним для будівництва та архітектури? – https://dia.dp.gov.ua/naskilki-shtuchnij-intelekt-mozhe-buti-korisnim-dlya-budivnictva-ta-arxitekturi.

3. Archimatica – https://archimatika.com/bim-technologies.

4. TEXTY.ORG.UA – https://texty.org.ua/fragments/110470/nazad-u-majbutnye-yak-shtuchnyj-intelekt-mozhe-zminyty-arhitekturu-pryklady-foto.

УДК: 623.746.5:629.7

АНАЛІЗ ТА ВИЗНАЧЕННЯ ВИМОГ ЩОДО ПОБУДОВИ КОНЦЕПЦІЇ РОБОТИ ДРОНІВ-ПЕРЕХОПЛЮВАЧІВ

Нижник Андрій, Партика Андрій
Національний Університет "Львівська політехніка", м. Львів

Метою даної роботи є аналіз та визначення вимог щодо побудови концепції роботи дронів-перехоплювачів. Дана розробка буде економічно вигідною та доцільною для знищення ворожих БПЛА оскільки вона ефективніша за зенітну артилерію, крім того ціна дрона перехоплювача буде в рази меншою ніж ціна ракети будь якого комплексу ППО, ПРО чи ПЗРК.

Ключові слова: Дрони перехоплювачі, FPV дрони, баражуючі боєприпаси, ППО, ПРО.

The purpose of this work is to analyze and determine the requirements for the construction of the concept of the operation of interceptor drones. This development will be economically beneficial and expedient for the destruction of enemy UAVs because it is more effective than anti-aircraft artillery, in addition, the price of an interceptor drone will be many times lower than the price of a missile of any air defense, anti-missile, or MANPADS complex.

Keywords: Interceptor drones, FPV drones, barrage ammunition, anti-aircraft defense, anti-missile defense.

Практика бойових дій показала гостру необхідність мати на озброєнні багато різних видів безпілотних літальних апаратів. Саме безпілотники допомагають зберегти людські життя, оскільки пілоти/оператори працюють віддалено, що зменшує ризики для життя.

Основна роль БПЛА полягає в забезпеченні розвідки, а також знищення живої сили противника, їх бронетехніки, укриттів, спостережних і вогневих точок. Крім того, вони мають різноманітне застосування, зокрема цілодобове патрулювання, доставку вантажів до важкодоступних районів, охорону об'єктів, коригування вогню артилерії, аеро- та фото розвідки, отримання актуальних просторових даних, радіоелектронної розвідки та для сигналів зв'язку[1].

Уже сьогодні можна стверджувати, що дрони будуть відігравати надважливу роль всіх наступних війнах та військових конфліктах. Вони не менш важливі ніж артилерія чи бронетехніка. Основні переваги дронів у порівнянні з іншими видами озброєння, наступні: вони досить малого розміру, не вимагають багато членів екіпажу, можуть знищити ціль, яка перевищує їхню ціну у тисячі разів[2]. Швидкість виготовлення нового БПЛА суттєво перевищує швидкість виготовлення бронетехніки Війна це завжди про економіку, про ефективне використання наявних ресурсів і про адаптацію економіки для роботи у важких умовах.

Основна частина

Зараз у всіх на слуху FPV дрони, розвідувальні дрони, ударні та морські дрони. Найбільш перспективним та малодослідженим є використання дронів для оборони, а саме для перехоплення та знищення ворожих дронів. Коли один дрон знищує інший, це по справжньому новий виток війни дронів. Найбільшою перевагою використання дронів перехоплювачів є те, що це швидкий, маневрений та дешевий спосіб знищення ворожого дрону. На відміну від традиційних засобів ППО, ПРО та ПЗРК, постріл яких коштує мільйони гривень, тому їх використання є економічно невигідним[3].

Концепція дронів перехоплювачів буде важливою ланкою у Армії дронів. Армія дронів – це спільний проєкт Міноборони, Мінцифри, Генштабу ЗСУ, Держспецзв'язку та UNITED 24.

Варто відмітити сфери застосування, де дрони перехоплювачі будуть максимально корисні та ефективні:

- знищенням розвідувальних дронів, щоб вони не могли навести ворожу артилерію на статичний об’єкт, який знаходиться під захистом або колону техніки, яка атакує;
- знищення ворожив дронів камікадзе та баражуючих боєприписав типу Ланцет, щоб захистити особовий склад та техніку на лінії зіткнення та у прифронтовій зоні.

Важливим елементом реалізації таких дронів-перехоплювачів є визначення вимог та концепції щодо їх роботи. В першу чергу варто зазначити наступні:

1. Розробка алгоритмів перехоплення та знищення дронів;
2. Розробка систем для виявлення ворожих дронів та оповіщення;
3. Покращення стійкості дрону до завад та розробка автономної системи керування дроном у випадку коли зв’язок з дроном буде все таки втрачено;
4. Покращення взаємодії дрону та оператора;
5. Збільшення енергоефективності та непомітності в повітряному просторі;

Після виявлення ворожогу дрону, його потрібно перехопити та знищити дроном перехоплювачем. Тут потрібно розрахувати траєкторію, та швидкість ворожогу дрону, щоб прокласти маршрут для його перехоплення. Із вдалим та швидким алгоритмом обчислення дрон перехоплювач може володіти гіршими льотними характеристиками, але бути здатним перехопити ціль.

Потрібна система, яка буде виявляти і сповіщати солдатів, що за ними веде спостереження ворожий дрон, для того щоб вони виконали всі необхідні дії. Дрона важко виявити традиційними радарами через його

малий розмір, але його легко виявити радіо-технічним військам, бо дрон - це пілотований літальний апарат, який приймає сигнали і відправляє телеметрію та відеосигнал з зворотному напрямку.

Дрон повинен бути стійким для засобі РЕБ. У це входить розробка нових протоколів передачі даних, а також впровадження штучного інтелекту, який може керувати дроном автономно. За допомогою цього можна автоматично захопити ціль та її знищити. У таких умовах дрон не буде випромінювати будь яких хвиль які притаманні відео передачі та сигналам керування дроном, отже його буде важче виявити та знищити.

Покращення взаємодії дрону та оператора. Потрібно розробити ПЗ для польотного контроллер, щоб він спрощував роботу пілота і підвищував ефективність ураження цілі. Дрони повинні здійснювати свою бойові вильоти за будь яких метеорологічних умов. Підготовка екіпажів повинна займати менше часу, все що може бути автоматизованим, має бути автоматизованим.

Реалізація всіх цих пристроїв та систем за допомогою різних алгоритмів та підходів повинна грунтуватись на спеціальному програмному забезпеченні, яке теж повинно відповідати всім вимогам безпеки та нормативним документам.

Висновки

Дрони перехоплювачі це перспективна система, яка дозволяє знешкоджувати ворожі БПЛА з мінімальними витратами. Стрілкова зброя малоефективна на великих відстанях і вимагає сторонню систему для виявлення та цілевказання на ворожий дрон.

Системи ППО, ПРО та ПЗРК надто дорого вартісні і ці системи логічно використовувати проти гвинтокрилів та літаків, де це економічно вигідно та обгрунтовано. Системи РЕБ надто великі, вимагають багато палива та енергії і відразу стають цілями для ворога. Випромінювання РЕБ можна відстежити за сотню кілометрів, тому його постійна робота неможлива, бо за координатами часто наносить удари авіація або артилерія.

Система здатна пасивно спостерігати за повітряним простором і дозволяє попередити персонал, про ворожий БПЛА, який за ними спостерігає чи збирається завдати удару. Також система може прийняти рішення і автоматично перехопити ворожий дрон.

Література

1. https://bdf.gov.ua/bezpilotnyky-pid-chas-viyny-zakonodavche-vrehuliuvannia-ta-vidpovidalnist-za-porushennia-povitrianoho-prostoru/
2. http://www.50northspatial.org/ua/civil-drones-during-wartime/
3. https://finance.ua/ua/goodtoknow/ppo2

УДК 004.736.56

ПЕРЕВАГИ ВИКОРИСТАННЯ БЛОКЧЕЙНУ У ДЕЦЕНТРАЛІЗОВАНИХ БАЗАХ ДАНИХ

Опірський Іван, Петрів Петро
Національний університет «Львівська політехніка»

Розглянуто ключові переваги блокчейну, що застосовуються для підвищення ефективності та безпеки в децентралізованих базах даних.
Ключові слова: блокчейн, децентралізовані бази даних, автоматизовані контракти

The key benefits of blockchain applied to improve efficiency and security in decentralized databases are considered.
Keywords: blockchain, decentralized databases, automated contracts

Метою цього дослідження є вивчення та оцінка використання блокчейн-технологій у децентралізованих базах даних, з акцентом на підвищення безпеки, ефективності та прозорості обробки даних.

У сучасному світі децентралізація даних – процес розподілу даних по мережі замість їх зосередження в одному місці – набуває все більшої актуальності, особливо в контексті забезпечення безпеки, надійності та прозорості інформації. Використання блокчейн технологій – розподілених баз даних, які забезпечують незмінність, прозорість та безпеку записів через криптографічне шифрування та консенсусні механізми – у базах даних відкриває нові можливості для створення міцних, безпечних та незмінних систем зберігання даних. Ці технології пропонують унікальні переваги, такі як децентралізація, захист від зовнішніх втручань та фальсифікацій, що робить їх важливим інструментом у сучасних інформаційних системах. Особлива актуальність розгляду цієї теми виникає у контексті зростаючих вимог до захисту даних та необхідності їх надійного зберігання і обробки.

Блокчейн технології в децентралізованих базах даних пропонують інноваційні та ефективні рішення, інтегруючи переваги незмінності, прозорості та безпеки в одну надійну систему. Ці технології забезпечують високий рівень захисту від несанкціонованих втручань та маніпуляцій з даними, що є критично важливим для будь-якого бізнесу. Завдяки децентралізованій природі блокчейну, дані розподіляються по мережі, знижуючи ризик централізованих збоїв та атак. Використання блокчейну в базах даних дозволяє підприємствам знизити загальні витрати на захист даних, одночасно підвищуючи їх надійність та доступність. Такий підхід не лише покращує безпеку даних, але й забезпечує вдосконалені можливості для управління та аудиту інформації, що стає ключовим фактором успіху в сучасному цифровому світі.

Технології блокчейну у децентралізованих базах даних включають в себе передові функції безпеки, які забезпечують комплексний захист від різноманітних кіберзагроз. Вони пропонують унікальний підхід до зберігання даних, включаючи криптографічне шифрування, розподілену архітектуру та механізми консенсусу для гарантії незмінності та прозорості даних. Ця методологія дозволяє захищати від внутрішніх та зовнішніх загроз, включно з маніпуляціями даними та несанкціонованим доступом. Використання блокчейну в базах даних створює захисний бар'єр, що запобігає атакам типу "відмова в обслуговуванні" (DoS) та іншим поширеним кібератакам. Блокчейн не тільки приховує внутрішню структуру бази даних від зовнішніх загроз, але й діє як ефективний механізм для контролю та управління доступом до даних, забезпечуючи високий рівень безпеки та надійності для корпоративних мережевих систем.

Блокчейн у децентралізованих базах даних має такі характеристики:

• Розподілена Архітектура. Блокчейн працює на основі розподіленої архітектури, що забезпечує розподіл даних по мережі, не залежачи від централізованих серверів чи систем. Це знижує ризики, пов'язані з централізованими атаками та збоями.

• Консенсусні Механізми. Для валідації та підтвердження транзакцій використовуються консенсусні механізми, як-от Proof of Work або Proof of Stake. Це гарантує, що всі записи в блокчейні є достовірними та затверджені більшістю мережі.

• Криптографічне Шифрування. Кожен блок даних у блокчейні захищений через криптографічне шифрування. Це робить блокчейн надзвичайно безпечним проти несанкціонованого доступу та маніпуляцій.

• Автоматизовані Контракти (Smart Contracts). Блокчейн дозволяє використовувати автоматизовані контракти, що діють на основі заданих умов та правил. Це підвищує ефективність та знижує можливість помилок чи фальсифікацій.

• Прозорість та Відстежуваність. Блокчейн забезпечує високий рівень прозорості, дозволяючи відстежувати кожну транзакцію в мережі, що підвищує довіру та відкритість системи. Переваги використання блокчейну у децентралізованих базах даних:

• Гарантована Незмінність Даних. Як тільки запис вноситься в блокчейн, він стає незмінним. Це означає, що жодна транзакція або блок даних, що не відповідає історії блокчейна, не може бути доданим або зміненим.

• Децентралізований Контроль. Всі транзакції в блокчейні підтримуються мережею рівноправних вузлів, забезпечуючи розподіл контролю та запобігання централізованим збоям і маніпуляціям.

• Захист від DoS-Атак. Розподілений характер блокчейна робить його стійким до DoS атак, забезпечуючи безперебійну роботу системи.

Отже, для забезпечення ефективного захисту децентралізованих баз даних, важливо використовувати передові технології, серед яких блокчейн виступає як ключовий компонент. Його унікальні властивості, такі як незмінність, децентралізація, прозорість та високий рівень безпеки, роблять його незамінним інструментом для захисту критично важливих даних в сучасному цифровому світі. Впровадження блокчейну в системи баз даних не тільки забезпечує надійний захист від зовнішніх та внутрішніх кіберзагроз, але й покращує загальну ефективність та надійність управління даними.

Література

1. Блокчейн як технологія децентралізованих баз даних / О. М. Сидоренко // Вісник Київського національного університету імені Тараса Шевченка. Серія "Комп'ютерні науки та інформаційні технології". – 2020. – Вип. 3(59). – С. 13-20.

2. Блокчейн-технологія в децентралізованих базах даних / В. В. Кісь, М. В. Піщак, І. О. Філіпчук // Вісник Національного університету "Львівська політехніка". Серія "Комп'ютерні науки". – 2022. – № 235. – С. 133-140.

3. Децентралізовані бази даних на основі блокчейн-технології / О. В. Мельник, О. В. Руденко // Вісник Одеського національного університету імені І. І. Мечникова. Серія "Математика. Комп'ютерні науки. Інформаційні технології". – 2021. – Вип. 35(2). – С. 103-110.

4. Блокчейн у децентралізованих базах даних: перспективи та виклики / О. І. Полотай, О. О. Тлумак // Вісник Національного університету "Львівська політехніка". Серія "Комп'ютерні науки". – 2023. – № 237. – С. 119- 128.

5. Блокчейн у системах управління даними: особливості та перспективи / В. В. Кісь, М. В. Піщак // Вісник Національного університету "Львівська політехніка". Серія "Комп'ютерні науки". – 2023. – № 238. – С. 137-146

УДК 004.42

ОСОБЛИВОСТІ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ МЕДИЧНИХ ДАНИХ ТА ЙОГО ВПЛИВ НА РЕАЛІЗАЦІЮ ПРОЕКТІВ ТРАНСФОРМАЦІЇ СУЧАСНОЇ ОХОРОНИ ЗДОРОВ'Я

Паньків Олег, Шолудько Роксолана
Львівський державний університет безпеки життєдіяльності

Подано особливості інтелектуального аналізу медичних даних та його вплив на реалізацію проектів трансформації сучасної охорони здоров'я. Проаналізована складові підвищення ефективності реалізації проектів щодо трансформації сучасної охорони здоров'я, а також зміни підходів до управління проектами у цій сфері. Проаналізовано сучасні засоби інтелектуального аналізу медичних даних та їх переваги під час використання у процесах медичних проектів.

Ключові слова: інтелектуальний аналіз, дані, медицина, проекти, трансформація

Features of intellectual analysis of medical data and its impact on the implementation of modern healthcare transformation projects are presented. The components of improving the efficiency of the implementation of projects related to the transformation of modern health care, as well as changes in approaches to project management in this area, are analyzed. Modern means of intellectual analysis of medical data and their advantages, when used in the processes of medical projects, are analyzed.

Keywords: intellectual analysis, data, medicine, projects, transformation

Інтелектуальний аналіз медичних даних стає все більшим використовуваним напрямком у сучасній медицині, привносячи нові можливості для діагностики, лікування та дослідження. Завдяки поєднанню передових технологій та аналізу великих обсягів інформації ми отримуємо можливість зрозуміти складні взаємозв'язки в медичних даних, які раніше залишилися непоміченими.

У нашій роботі представлено особливості інтелектуального аналізу медичних даних, його переваги та виклики. Вивчення цього напряму не лише сприяє розвитку нових методів управління проектами лікування пацієнтів, а й дозволяє зробити медичну практику більш ефективною та персоналізованою. Розглянемо, як інтелектуальний аналіз даних у медицині може вплинути на проекти розвитку сучасної охорони здоров'я.

Інтелектуальний аналіз даних у медицині відкриває широкі можливості для підвищення ефективності реалізації проектів щодо трансформації сучасної охорони здоров'я, а також зміни підходів до управління проектами у цій сфері. На рис. 1 наведено вплив інтелектуального аналізу медичних даних на трансформації сучасної охорони здоров'я.

Рисунок 1 – Вплив інтелектуального аналізу медичних даних
на трансформації сучасної охорони здоров’я

Вплив інтелектуального аналізу медичних даних на персоналізоване лікування проявляється через те, що він дозволяє аналізувати великі обсяги клінічних та генетичних даних, щоб розуміти індивідуальні особливості пацієнтів. Це дозволяє розробляти персоналізовані стратегії лікування, враховуючи генетичні особливості, стан здоров'я та інші фактори.

Стосовно превентивної медицини, то інтелектуальний аналіз даних забезпечує раннє виявлення факторів ризику та здійснення точних прогнозів для конкретних видів захворювань. Це дозволяє у системі охорони здоров'я отримати першочергові заходи для запобігання захворюванням та підвищення ефективності медичних проектів із їх профілактики.

Оптимізація лікарської допомоги завдяки інтелектуальному аналізу медичних даних забезпечує вдосконалення процесів підтримки прийняття рішень у медичних установах, надаючи лікарям рекомендації на основі обробки великих обсягів даних. Це полегшує точну діагностику, вибір оптимальних методів лікування та покращення результатів лікування хвороби.

Під час дослідження нових методів та лікарських засобів інтелектуальний аналіз великих обсягів клінічних даних забезпечує ідентифікацію нових тенденцій, знаходження взаємозв'язків між ними та встановлення нових можливостей для досліджень. Це дозволяє вченим та фармацевтичним компаніям ефективно розробляти нові методи лікування та лікарські засоби.

Інтелектуальний аналіз даних забезпечує ефективне управління ресурсами, що скорочує зайві витрати та забезпечує оптимізацію роботи медичних установ. Штучний інтелект та аналітичні системи дозволяють прогнозувати попит на медичні послуги, управляти запасами медикаментів та ефективно розподіляти персонал за заданого стану проектного середовища.

Інтелектуальний аналіз даних є інструментом для моніторингу захворювань та виявлення епідемій. Він дозволяє оперативно аналізувати великі масиви даних з різних джерел, щоб своєчасно реагувати на захворювання та вживати необхідні заходи з контролю та профілактики.

Інтелектуальний аналіз даних медичних даних забезпечує підвищення якості медичних послуг завдяки впровадженню системи оцінки якості медичних послуг та покращення взаємодії між пацієнтами та медичним персоналом. Це дозволяє створити більш прозору та ефективну систему надання медичної допомоги.

Вцілому, інтелектуальний аналіз даних в медицині є ключовим інструментом для розвитку сучасної охорони здоров'я через реалізацію низки проектів, що сприяє отримання точної діагностики та лікування пацієнтів, а також забезпечує ефективне управління реалізацією розвитку системи охорони здоров'я. Завдяки цьому підходу ми можемо досягти більш високої ефективності та персоналізації в наданні медичних послуг та підвищення рівня лікування пацієнтів (табл. 1).

Інтелектуальний аналіз медичних даних має широкий спектр застосувань у медичних проектах. Він може використовуватися для прогнозування захворювань, оцінки ефективності лікування, управління лікуванням та діагностикою, персоналізованої медицини та генетичної терапії, автоматизації діагностики та аналізу зображення, а також контролю захворювань та глобального епідемічного аналізу. Таким чином, інтелектуальний аналіз медичних даних є перспективним напрямом розвитку медицини, який має потенціал для значного покращення якості медичної допомоги та результатів лікування.

За допомогою машинного навчання та аналітики даних здійснюється точне прогнозування ризиків розвитку захворювань із врахуванням таких чинників, як вік, стать, генетичні особливості, спосіб життя, медична історія пацієнтів тощо. Це допомагає лікарям виявити захворювання на ранніх стадіях та можливість розпочати його лікування, коли воно є найбільш ефективним.

За допомогою автоматизованих систем прийняття рішень оцінюється ефективність лікування на основі даних про стан пацієнтів, результати лабораторних досліджень, показники роботи медичного обладнання тощо. Це значно допомагає лікарям оптимізувати процеси лікування та досягти найкращих результатів для пацієнтів.

Штучний інтелект використовується для автоматизації завдань, пов'язаних з лікуванням та діагностикою, а також призначення препаратів, складання планів лікування, інтерпретація результатів лабораторних досліджень тощо. Це допомагає лікарям зменшити час на діагностику, який можна використати для більш складних завдань та забезпечити пацієнтам більш якісну медичну допомогу.

Таблиця 1

Засоби інтелектуального аналізу медичних даних та їх переваги під час використання у процесах медичних проектів

Засіб інтелектуального аналізу даних	Процеси медичних проектів	Переваги
Машинне навчання та аналітика	Прогнозування захворювань та оцінення ефективності лікування	✓ Раннє виявлення ризиків та індивідуальне лікування ✓ Оптимізація розподілу ресурсів ✓ Покращення результатів лікування
Автоматизовані системи прийняття рішень	Управління лікуванням та діагностикою	✓ Пришвидшення та зростання точності прийняття рішень ✓ Зменшення ймовірності помилок ✓ Підтримка прийняття рішень у виборі оптимальних методів лікування
Системи аналізу геномних даних	Персоналізована медицина та генетична терапія	✓ Розробка індивідуальних стратегій лікування ✓ Виявлення генетичних причин захворювань ✓ Оптимізація лікування із врахуванням генетичних особливостей
Штучний інтелект у медичних діагностиках	Автоматизація діагностики та аналізу зображення	✓ Зменшення часу діагностики ✓ Підвищення точності діагнозу захворювання ✓ Вдосконалення роботи медичного обладнання
Системи моніторингу та прогнозування епідемій	Контроль захворювань та глобальний епідемічний аналіз	✓ Раннє виявлення та прогнозування епідемій ✓ Поліпшення глобального здоров'я та безпеки населення ✓ Ефективне управління ресурсами в умовах кризи

Системи аналізу геномних даних використовуються для розробки індивідуальних стратегій лікування, враховуючи генетичні особливості пацієнтів. Це забезпечує пацієнтам більш ефективне лікування та скорочує час одужання.

Системи моніторингу та прогнозування епідемій можуть використовуються для раннього виявлення та прогнозування епідемій. Це допомагає у розробці ефективних заходів для контролю захворювань та захисту населення.

Інтелектуальний аналіз медичних даних є швидко розвиваючою галуззю, яка має потенціал для значного впливу на медицину. Застосування цих технологій допомагає покращити якість медичної допомоги, підвищити ефективність проектів лікування та забезпечити пацієнтам здоров'я за меншого часу лікування.

Література

1. Malanchuk, O., Tryhuba, A., Tryhuba, I., Bandura, I. A conceptual model of adaptive value management of project portfolios of creation of hospital districts in Ukraine. *CEUR Workshop Proceedings*. 2023; 3453, 82–95.

2. Tryhuba, A., Malanchuk, O., Tryhuba, I. Prediction of the Duration of Inpatient Treatment of Diabetes in Children Based on Neural Networks. *CEUR Workshop Proceedings*. 2023; 3426, 122–135.

3. Tryhuba A., Malanchuk O., Tryhuba I. Prediction of the Duration of Inpatient Treatment of Diabetes in Children Based on Neural Networks. *Proceedings of the Modern Machine Learning Technologies and Data Science Workshop (MoMLeT&DS 2023)*. 2023; 122-135.

УДК 004.9

РОЗРОБКА ВЕБ-ДОДАТКА ДЛЯ ПОКРАЩЕННЯ ОРГАНІЗАЦІЇ ЗАХОДІВ ТЕНІСНОЇ СПІЛКИ ЛЬВОВА

Пенькова Дар'я
Львівський національний університет імені Івана Франка, м. Львів

Мета роботи – створення нового веб-застосунку для тенісної спілки Львова з можливістю розміщень там оголошень про тренування та проведення любительських турнірів.

Ключові слова: веб-застосунок, ASP.NET, Angular.

The purpose of the work is to create a web application for the Lviv Tennis Community with the ability to post training sessions and organize amateur tournaments.

Keywords: web application, ASP.NET, Angular.

Великий теніс – одна з найбільш широко розповсюджених і впізнаваних спортивних ігор. За даними ЮНЕСКО в кінці XX століття він посів перше місце серед інших видів спорту за масштабністю і швидкістю розвитку спортивних заходів. Не винятком став і Львів, де також активно розвивався великий теніс.

Не зважаючи на вище сказане, сьогодні, у технологічному XXI столітті, відчувається брак належних сучасних застосунків для тенісної спілки Львова. Особливою проблемою є пошук партнерів для проведення індивідуальних або ж групових тренувань та організація любительських турнірів. Саме тому метою цієї роботи є створення нового веб-застосунку для тенісної спілки Львова, що міститиме в собі такий функціонал:

- можливість розміщення оголошення про тренування з вказанням часу, дати, місця, спортивного рівня та кількості людей;
- можливість для зареєстрованих користувачів відгукуватись на оголошення задля комунікації з їх організатором і подальшим успішним проведенням тренувань;
- можливість створення невеликих спортивних заходів на кшталт любительських турнірів.

Для реалізації проекту було обрано низку найсучасніших технологій та інструментів.

Для розробки застосунку використовувався ASP.NET Core [1], Entity Framework Core [2] для роботи з даними та доступу до них. На стороні фронтенду Angular [3] з використанням Typescript та Angular material [4] для створення інтерфейсу – бібліотека, що містить в собі вже готові рішення для деяких компонентів інтерфейсів.

В додатку також була реалізована система оповіщення користувачів про дії в додатку, такі як: сповіщення про заявку нового користувача на тренування/турнір, зміна статусу користувача, що подався на подію, результати зіграних матчів та турніру загалом. Для цього використовувався SMTP (Simple Mail Transfer Protocol) клієнт - програмне забезпечення або клієнтський компонент, який використовується для відправлення електронної пошти через сервер SMTP. SMTP є стандартним протоколом для передачі електронних листів по мережі Інтернет.

Висновки. В ході проведення аналізу існуючих додатків було з'ясовано, що ще не існує хорошого додатку, який би повністю задовольняв всі потреби львівських тенісистів. Тому було прийнято рішення про створення нового веб-додатку. За допомогою обраного стеку технологій вдалось реалізувати весь базовий функціонал програми.

Література

1. ASP.NET Core documentation : веб-сайт. URL: https://learn.microsoft.com/en-us/aspnet/core/introduction-to-aspnet-core?view=aspnetcore-6.0
2. Entity Framework Core Microsoft Documentation : веб-сайт. URL: https://docs.microsoft.com/en-us/ef/core/
3. Angular documentation : веб-сайт. URL: https://angular.io/docs
4. Angular Material documentation: веб-айт. URL: https://material.angular.io/

УДК 614.8

ПРИКЛАДНЕ ПРОГРАМУВАННЯ РОЗРАХУНКУ ВНУТРІШНЬОГО ПРОТИПОЖЕЖНОГО ВОДОПРОВОДУ БАГАТОФУНКЦІОНАЛЬНОЇ БУДІВЛІ

Петухова Олена, Білаш Євгеній, Бєрмант Дарина, Добринська Валерія
Національний університет цивільного захисту України, м.Харків

Розрахунок внутрішнього протипожежного водопроводу (ВПВ) виконується при його проєктуванні. Для оптимізації процесу розрахунку, можливості оцінки декількох варіантів влаштування ВПВ існують програмні комплекси недоліком яких є можливість роботи з будівлями конкретного призначення – житловими, громадськими або виробничими. В роботі обґрунтовано створення програмного комплексу з розрахунку ВПВ багатофункціональної будівлі.

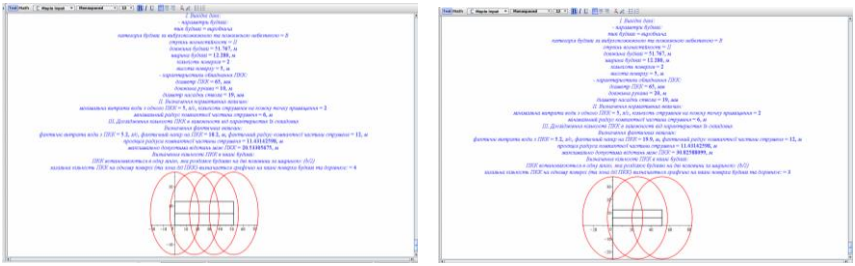
Ключові слова: внутрішній протипожежний водопровід, програмний комплекс

The calculation of the internal fire watersupply (IFW) is performed during its design. In order to optimize the calculation process, the possibility of evaluating several options for installation of IFW, there are software complexes, the disadvantage of which is the ability to work with buildings of a certain purpose – residential, public or industrial. The work substantiates the creation of a software complex for calculating the IFW of a multifunctional building.

Keywords: internal fire watersupply, program complex, multi-functional building

Внутрішній протипожежний водопровід є складовою системи протипожежного захисту будівель, призначений для ліквідації або локалізації пожеж в середині будівель в найкоротший термін, як правило до прибуття підрозділів пожежної охорони. Можливість ВПВ забезпечити подачу необхідної кількості води з необхідним тиском, що є умовою успішного його використання, створюється на стадії проєктування [1]. Вимоги сучасних нормативних документів передбачають створення умов ефективної роботи ВПВ, але кожне рішення може мати декілько варіантів.

Розрахунок ВПВ складається з наступних етапів: визначення нормативних величин та їх фактичних значень для заданої будівлі; розрахунок необхідної кількості пожежних кран-комплектів та визначення місць їх розташування в плані будівлі; трасування водопровідної мережі таким чином, щоб до кожного ПКК вода подавалась найкоротшим шляхом; визначення необхідного тиску на введенні в будівлю та вибір схеми ВПВ (з підвищувальними установками або без них) [1-3]. Кожний етап може мати декілько варіантів рішень, що може вплинути на ефективність використання ВПВ при гасінні пожежі [4]. Використання програмних комплексів значно спрощує процес аналізу багатьох рішень та прийняття остаточного обґрунтованого варіанту (рис.1).



а) б)

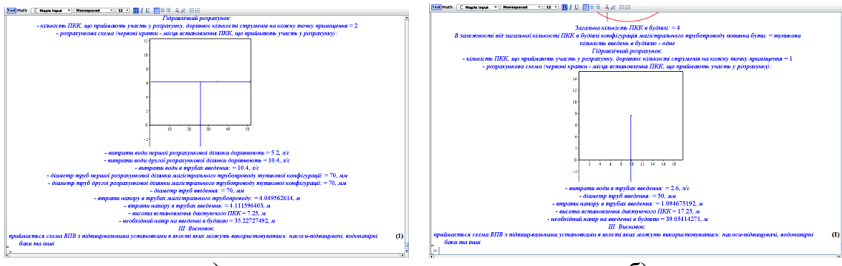
Рисунок 1 – Приклад використання програмного комплексу “ВПВ” для розрахунку для заданої будівлі кількості ПКК, що мають довжину рукава: а) 10 м; б) 20 м

Комплекс “ВПВ” з успіхом використовується в освітньому процесі, в практичній діяльності працівниками підрозділів пожежної охорони при перевірці об'єктів на дотримання вимог пожежної безпеки, проєктувальниками; але використання комплексу доцільно лише для будівель конкретного призначення – житлових, громадських або виробничих. На теперішній час більшість будівель складаються з декількох різних за призначенням частин, тобто виконують одночасно багато функцій – є багатофункціональними. Відмінності в призначенні окремих частин будівлі обумовлює різницю у нормативних витратах на пожежогасіння та кількості струменів, що необхідно подавати від пожежних кран-комплектів на кожну точку приміщення для успішного пожежогасіння. А це значно впливає на результат всіх етапів проєктування та розрахунку.

Було запропоновано послідовне використання програмного комплексу для кожної окремої частини будівлі, що має неоднакове призначення. Результат розрахунку показав, що можливо лише визначити фактичні характеристики ПКК. Тобто фактично мета розрахунку ВПВ (визначення необхідного напору на введенні, вибір схеми ВПВ) не досягається використанням комплексу та проєктувальникам необхідно власноруч виконувати подальші розрахунки, послідовно перебираючи декілька можливих варіантів.

Був виконаний розрахунок ВПВ будівлі, яка складається з триповерхової частини адміністративно-побутового призначення та двоповерхової частини складського призначення. Результати без використання програмного комплексу показали, що подачу води в середину будівлі можна забезпечувати за допомогою одного введення, при цьому магістральний трубопровід може мати тупикову конфігурацію, тому що загальна кількість пожежних кран-комплектів менше 12 (6 ПКК в складській частині та 4 ПКК в адміністративно-побутовій частині). Схема ВПВ для будівлі повинна бути з підвищувальними установками, тому що за розрахунком необхідний напір на введенні в будівлю склав 36,8 м, а гарантований напір у зовнішній мережі за даними дорівнює 30 м.

Розрахунок за допомогою програмного комплексу ВПВ був виконаний послідовно для кожної частини будівлі окремо (рис.2) та одержані результати відрізнялись від самостійних розрахунків.



а) б)

Рисунок 2 – Результат розрахунку за допомогою програмного комплексу “ВПВ” багатофункціональної будівлі: а) складської частини; б) адміністративно-побутової частини

Аналіз результатів розрахунків з використанням програмного комплексу та без нього дозволяє зробити висновок, що використання програмних комплексів для проєктування ВПВ складних за призначенням будівель доцільно та ефективно за умовами врахування особливостей таких будівель при програмуванні відповідних комплексів.

Література

1. ДБН В.2.5-64:2012 Внутрішній водопровід та каналізація. [Чинний від 013-03-01]. Київ: Мінрегіон України, 2013. 134 с.

2. Петухова О.А., Андронов В.А., Горносталь С.А., Черепаха Р.Е. Протипожежне водопостачання: Підручник – Харків. – Друкарня Мадрид, 2022. – 280 с. URL: http://moodle.nuczu.edu.ua/mod/folder/view.php?id=4339.

3. Петухова О. А., Горносталь С. А., Щербак С. М., Левенко Г. М. Розробка підходу до розташування пожежних кран-комплектів в плані будівлі. Problems of Emergency Situations. 2021. № 2(34) С. 154-167 DOI: https://doi.org/10.52363/2524-0226-2021-34-12. URL: http://repositsc.nuczu.edu.ua/handle/123456789/14721.

4. Petukhova O., Cherepakha R., Dobrynska V., Kulesh D. Дослідження характеристик пожежних кран-комплектів театрів // Scientific progress: innovations, achievements and prospects. Proceedings of the 7th International scientific and practical conference. MDPC Publishing. Munich, Germany. 2023. Pp. 231-237. URL: https://sci-conf.com.ua/vii-mizhnarodna-naukovo-praktichna-konferentsiya-scientific-progress-innovations-achievements-and-prospects-3-5-04-2023-myunhen-nimechchina-arhiv/.

УДК 004.072.2+655.532

ФАКТОРИ ЯКОСТІ ПРОЦЕСУ ЗРУЧНОСТІ ЧИТАННЯ ЕЛЕКТРОННИХ ВИДАНЬ

Пітушенко О. А., Сельменська З.М.
Українська академія друкарства

У роботі представлено та обґрунтовано характеристики та фактори, які впливають на зручність читання електронних видань з урахуванням взаємозв'язків між ними та дослідженими ваговими значеннями, як засобом реєстрації, зберігання і поширення знань у контексті глобалізації розвитку електронних видань у сфері освіти.

Ключові слова: шрифт; зручність читання; якісні характеристики; ієрархічні структури; фактори пріоритетності.

The report presents and justifies the characteristics and factors influencing the readability of electronic publications, taking into account the relationships between them and the investigated weighting values, as a means of registering, storing, and disseminating knowledge in the context of the globalization of electronic publication development in education.

Keywords: font, readability, qualitative characteristics, hierarchical structures, priority factors.

У контексті глобалізації розвитку людства реєстрація, зберігання і поширення знань є актуальною науковою проблемою. Беззаперечно можна чітко виділити проблематику якісного шрифтового оформлення друкованих та електронних видань. Правильний добір шрифтового оформлення залежить від багатьох об'єктивних факторів і в свою чергу впливає на те, наскільки легко можна освоїти будь яку інформацію. Основним завданням будь якого шрифта в електронному чи фізичному виданні є: досягнення максимальної універсальності донесення інформації. Різне шрифтове оформлення часто застосовують у формі зручного інструменту для різного вікового сегменту читача, під час планування та прийняття рішень стосовно відповідності до певних критеріїв, а також визначення розбірливості. Термін розбірливості шрифту означає, наскільки легко розпізнати будь яку букву на сторінці [1]. Тому слід зазначити, що для вирішення прикладних задач виникає потреба адаптації інформації способом логічних математичних конструкцій виражених на основі теорії графів.

Теорія графів у математиці займається вивченням особливого виду математичних структур – графів, що використовуються для моделювання парних відношень між об'єктами. Графи у цьому контексті складаються з вершин (точок), які з'єднані ребрами (лініями) [2].

Нехай сукупність факторів становить деяку множину H = {h1, h2, …, hn}. Виберемо з цієї сукупності підмножину H1 ∈ H найбільш суттєвих факторів. Для наочності зроблено математичне позначення його мнемонічною назвою: h1 – гарнітура шрифту – ГШ; h2 – кегель шрифту – КШ; h3 – довжина рядка – ДР; h4 – інтерліньяж шрифту – ІШ; h5 – насиченість шрифту – НШ; h6 – накреслення шрифту – НАШ; h7 – колір текстового оформлення електронного видання – КТ; h8 – швидкість читання тексту електронного видання – ШЧ; h9 – складність тексту електронного видання – СТ; h10 – колір фону електронного видання – КФ; h11 – розмір текстового блока електронного видання – РТБ; h12 – види електронних видань – ВЕВ; h13 – параметри вивідного пристрою – ПВП;

Таким чином підмножину факторів H1 та можливий взаємовплив між ними подано у вигляді орієнтованого графу (рис. 1). На вершинах розміщено підмножини H_1, а ребрами з'єднанні сусідні вершини для яких визначений зв'язок що вказує на залежність фактора. На основі графу будуємо бінарну матрицю залежності B для множин вершин H.

Вершину hi називають досягнутою з вершини hj, якщо в орієнтованому графі існує шлях з hj до hi. Позначимо підмножину досягнутих вершин через R(hi). Вершину hj називають попередницею вершин hi, якщо можливе досягнення hi із h.

Взявши множини таких вершин A(hi) = R(hi) ∩ A(hi), для яких виконується умова недосяжності з будь-яких з вершин, що залишились множини H, може бути визначена як рівень ієрархії.

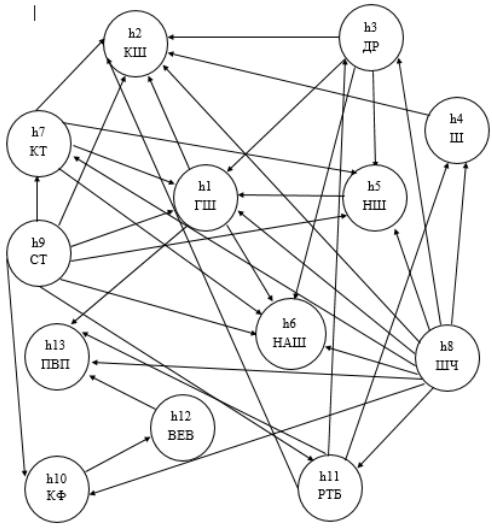


Рисунок 1

Для формування підмножини A(hi) із і-го стовпця матриці досяжності виписуються номери тих елементів, які мають одиниці. Підмножина R(hi) ∩ A(hi) формується як логічний перетин елементів підмножини R(hi) та A(hi). За допомогою постійних ітерацій проводиться постійне розподілення факторів впливу. Було отримано ієрархічно структуровану модель (рис. 2), що в свою чергу буде встановлювати пріоритетність впливу розглянутої сукупності факторів на зручність читання тексту в електронних виданнях.

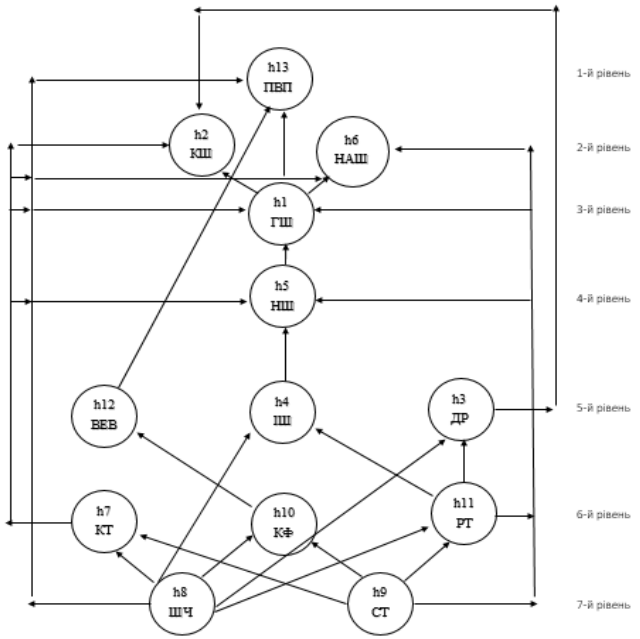


Рисунок 2

Отже, на основі теорії графів побудовано структуровану ієрархічну модель з виявленням пріоритетності факторів впливу на якісні показники електронних видань. Це дало змогу виокремити основні фактори зручності читання текстового матеріалу за ступенем впливу, розділити їх на сім основних рівнів та враховувати їх при оптимізації алгоритму системи.

Література

1. Васюта, С.П., Хамула, О.Г., & Куць, Я.Й. (2020). Технологічні особливості створення шрифтів для електронних видань: монографія. Львів: Українська академія друкарства.

2. Теорія графів : навч. посіб. для здобувачів ступеня бакалавра за освітньою програмою «Комп'ютерний моніторинг та геометричне моделювання процесів і систем» спеціальності 122 «Комп'ютерні науки»/ І.М. Кузьменко; КПІ ім. Ігоря Сікорського. —Київ: КПІ ім. Ігоря Сікорського, 2020. — 71 с).

УДК 004.75

КОНЦЕПЦІЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СФЕРІ ОСВІТИ

Побережник Василь, Балацька Валерія, Опірський Іван
Національний Університет «Львівська політехніка», м. Львів, Україна

Анотація: в даній роботі розглядається можливість застосування технологій блокчейн, смарт контрактів та NFT в контексті сфери надання освітніх послуг. Пропонується концепція системи яка дозволить автоматизувати створення цифрової версії диплому та спростити перевірку на достовірність таких дипломів зацікавленими сторонами.
Ключові слова: блокчейн, NFT, смарт контракти, освіта

Abstract: this paper considers the possibility of applying blockchain technologies such as smart contracts and NFT in the context of the educational services providing. The concept of a system that will allow to automate the creation of a digital version of a diploma and to simplify the verification of the authenticity of such diplomas by interested parties is proposed.
Keywords: blockchain, NFT, smart contracts, education

Використання технології блокчейн вийшло за межі використання у сфері операцій з криптовалютами та їхнього майнінгу. На сьогоднішній день застосування технології можна побачити в таких сферах як медицина, логістика тощо [1]. Однак, в контексті надання освітніх послуг, науковий інтерес становлять такі блокчейн технології як смарт-контракти та NFT і, зокрема, сам блокчейн.

Смарт контракти — це програмний код, який після завантаження в блокчейн мережу автоматично виконується після того, як виконаються певні умови задані у цьому контракті [2].Однією з переваг цієї технології є те, що сторонам, які уклали такий смарт-контракт не потрібно залучати третю сторону, що дозволяє автоматизувати процес проведення угоди, наприклад обміну криптовалюти, створення NFT, а також те, що результат дії такого смарт-контракту буде записаний в блокчейн мережу, що унеможливить його несанкціоновану зміну.

NFT — це невзаємозамінні криптографічні токени. Одним із помилкових уявлень про NFT є те, що вони використовуються лише для операції купівлі чи продажу цифрового мистецтва [3]. Втім, їхнім основним призначенням є їхнє застосування для підтвердження власності над цифровими активами [4], наприклад авторство фото, захист медіа файлів від незаконного використання [5] тощо.

Зважаючи на властивості згаданих технології, можна припустити їхнє застосування в сфері надання освітніх послуг. Основними характеристиками, які буде забезпечувати така система будуть цілісність та незмінність даних, а сама система буде надавати можливість автоматичної видачі їм сертифікатів чи дипломів та забезпечення доступу для їхньої верифіка-

ції. Однією з важливих умов є використання мережі блокчейн гібридного типу, оскільки вона дозволить контролювати додавання нових вузлів, що не доступно відкритій мережі, а також дозволить отримувати лише дозволену інформацію для зовнішніх користувачів, залишаючи чутливі дані всередині мережі у захищеному стані.

Варто зазначити, що негативним фактором, який може істотно впливати на реалізацію та підтримку такої системи є ціна смарт контрактів, яка має пряму залежність від розміру коду завантаженого в мережу [6] і, відповідно, робить сценарії із використанням складних контрактів дороговартісними, що буде безпосередньо впливати на ціну реалізації такої системи і на вартість надання самих освітніх послуг.

Принцип роботи системи буде полягати в тому, щоб використати смарт контракт для генерації цифрової версії диплому, роль якої відіграватиме NFT та буде збережений у мережі блокчейн з метою захисту від несанкціонованих змін. На рис. 1 зображено концептуальну схему такої системи. Її принцип роботи полягає в тому, що отримувач освітніх послуг укладає смарт контракт із надавачем таких послуг, та розпочинає освітній процес. Надавач освітніх послуг вносить у мережу академічні дані студента, наприклад інформацію про успішний захист диплому. Смарт контракт аналізує стан мережі блокчейн та визначає правдивість виконання умов видачі цифрового диплому, наприклад згаданий раніше запис в блокчейні про успішний захист. Коли така умова виконується, то смарт контракт генерує NFT-диплом, додаючи туди необхідну інформацію для ідентифікації власника та зберігає його у мережі блокчейн, встановлюючи власником диплома отримувача освітніх послуг, який успішно завершив освітній процес.

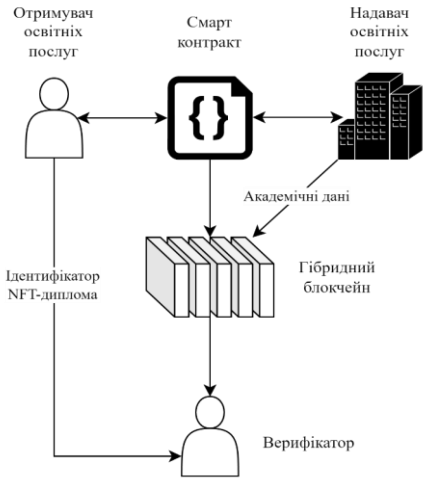


Рисунок 1 – Концептуальна схема системи

За необхідності власник NFT-диплому надає ідентифікатор верифікатору, який зможе перевірити справжність диплому перевіривши відкриту частину гібридного блокчейну. Прик використанні даного підходу необхідно забезпечити можливість однозначно підтвердити особу та право власності даним NFT без можливого розкриття персональної інформації широкому загалу. Виходом із цієї ситуації може стати гешування ідентифікаторів особи з метою використання отриманого гешу, як ідентифікатора власника.

Хоч така система виглядає привабливою в контексті використання нових технологій та підтвердження кваліфікації через підтвердження здобутих знань, її використання на даному етапі розвитку технології блокчейн, зважаючи на її недоліки[7] є, радше, можливим доповненням до наявних систем.

Література

1. 26 top blockchain applications and use cases in 2023. Learn Hub | G2. URL: https://learn.g2.com/blockchain-applications (дата звернення: 22.11.2023).

2. What are smart contracts on blockchain? | IBM. IBM in Deutschland, Österreich und der Schweiz | IBM. URL: https://www.ibm.com/topics/smart-contracts (дата звернення: 21.11.2023).

3. Lian A. NFTs Don't Work The Way You Might Think: Misconceptions About NFTs | HackerNoon. HackerNoon - read, write and learn about any technology. URL: https://hackernoon.com/nfts-dont-work-the-way-you-might-think-misconceptions-about-nfts (дата звернення: 21.11.2023).

4. Non-fungible Token (NFT) | Definition, How to Create and Sell. Finance Strategists. URL: https://www.financestrategists.com/wealth-management/cryptocurrency/nonfungible-tokens (дата звернення: 21.11.2023).

5. Poberezhnyk V., Harasymchuk O., Opirskyy I. Ochrona plików multimedialnych przed fałszowaniem i nielegalnym wykorzystaniem w oparciu o blockchain. Przetwarzanie, transmisja i bezpieczeństwo informacji. 2022. С. 107–118. URL: https://doi.org/10.53052/9788367652001.09 (дата звернення: 22.11.2023).

6. How much does it cost to deploy a smart contract on ethereum?. Doubloin. URL: https://www.doubloin.com/learn/costs-deploy-smart-contract (дата звернення: 22.11.2023).

7. Top disadvantages of blockchain technology. 101 Blockchains. URL: https://101blockchains.com/disadvantages-of-blockchain/ (дата звернення: 22.11.2023).

УДК 004.71

АНАЛІЗ ФУНКЦІОНАЛЬНИХ ОСОБЛИВОСТЕЙ КОМУТАТОРА CISCO C9300-48P-E

Потапенко Олександр, Бурак Назарій
Львівський державний університет безпеки життєдіяльності

Комутатори є ключовим елементом мережевої інфраструктури, відіграючи важливу роль у забезпеченні ефективної та безперебійної передачі даних в сучасних мережах. Проаналізовано функціональні особливості комутатора Cisco C9300-48P-E. Виконано аналіз переваг та недоліків їх використання.

Ключові слова: комп'ютерна мережі, порти, маршрутизація, продуктивність

Switches are a key element of network infrastructure, playing an important role in ensuring efficient and uninterrupted data transmission in modern networks. Analysed functional features of the Cisco C9300-48P-E switch. Were highlighted its advantages and disadvantages of use.

Keywords: computer networks, ports, routing, performance

У сучасному світі комп'ютерні мережі забезпечують обмін інформацією між усіма пристроями на різних географічно розміщених об'єктах. За допомогою використання різних середовищ та стандартів передачі даних відбувається циркуляція даних як загального інформаційного, так і спеціального службового призначення. Забезпечення надійності та швидкості обміну є важливою та необхідною умовою роботи сучасних інформаційних систем. Одним із компонентів комп'ютерних мереж, який організовує та керує взаємодією різних сегментів мережі на рівні розподілу є комутатор. Розуміння його принципів роботи, особливостей налаштування та базових апаратних реалізацій дозволить побудувати ефективну топологію мережі.

У даному дослідження виконано аналіз мережевого комутатора компанії Cisco – Cisco C9300-48P-E(Рис 1.). З метою виконання грунтовного огляду, виокремлено основні шість характеристик, які доцільно детально розглянути, зокрема : порти та пропускна задтність, продуктивність і швидкість передачі даних, управління, розширюваність, сумісність та енергоефективність.

Рисунок 1 – К омутатор Cisco C9300-48P-E

Детально розглянемо кожен із обраних напрямів аналізу.

1. Порти і пропускна здатність: комутатор обладнаний 48 портами, що дозволяє підключити значну кількість кінцевих пристроїв. Це особливо корисно в сучасних офісних середовищах, де збільшується кількість мережевих пристроїв. Кожен порт підтримує технологію PoE(Power over Ethernet), що робить його ідеальним вибором для підключення IP-камер, телефонів та інших пристроїв, які вимагають живлення через мережевий кабель. Щодо пропускної здатності, комутатор забезпечує високошвидкісну передачу даних, оптимізуючи мережевий трафік та запобігаючи його перевантаженню.

2. Продуктивність і швидкість передачі даних: висока продуктивність комутатора обумовлена не лише кількістю портів, але й використанням сучасних технологій обробки даних. Забезпечуючи швидкість передачі даних на рівні, що відповідає сучасним стандартам, цей комутатор стає надійним рішенням для бізнес-середовищ, де вимагається миттєвий доступ до інформації. Із застосуванням технологій високошвидкісного комутування, комутатор Cisco C9300-48P-E дозволяє оптимізувати роботу мережі, зменшуючи час передачі даних і забезпечуючи ефективне використання доступної пропускної здатності. Застосування стандартів безпеки, таких як 802.1X, надає можливість автентифікації пристроїв в мережі, пропускаючи у внутрішній сегмент мережі лише авторизовані пристрої. Такий підхід ефективно захищає мережеві ресурси від несанкціонованого доступу і збільшує загальний рівень безпеки мережі від атак, таких як перехоплення даних або зміни конфігурації пристроїв.

3. Управління: комутатор використовує розширений набір засобів управління, що спрощує конфігурацію та моніторинг мережі. Він підтримує різні інтерфейси для віддаленого управління, включаючи SSH та SNMP, що надає адміністраторам можливість віддалено контролювати та налаштовувати параметри комутатора,. Забезпечення доступу до конфігурації через інтерфейси командного рядка та графічний інтерфейс користувача забезпечує просте та зрозуміле управління комутатором. Такий підхід до управління дозволяє максимально використовувати функціонал комутатора та легко впроваджувати необхідні зміни в конфігурації мережі.

4. Розширюваність: комутатор володіє високим рівнем розширюваності, яка є важливим аспектом в забезпеченні майбутньої готовності мережі до росту. Однією з ключових характеристик є сумісність з різноманітними модулями розширення. Наявність слотів для додаткових модулів, таких як SFP (Small Form-Factor Pluggable), дозволяє збільшувати можливості мережі, зокрема, підключати пристрої за допомогою оптичного волокна для підтримки великих відстаней передачі. Це забезпечує гнучкість і можливість адаптації до зростаючих потреб мережі, а також дозволяє впроваджувати нові технології та сервіси без необхідності повного змінення обладнання.

5. Сумісність: комутатор сумісний із світовими стандартами мережевого обладнання. Зокрема, він підтримує широкий спектр стандартів, таких як IEEE 802.3, які визначають правила функціонування Ethernet-мереж. Це гарантує його взаємодію із різноманітними мережевими пристроями, що використовуються у сучасних корпоративних середовищах. Сумісність із стандартами є важливим аспектом при будівництві мережі, оскільки вона забезпечує інтероперабельність між різними виробниками обладнання, стабільність та надійність функціонування.

6. Енергоефективність: комутатор використовує інтелектуальні механізми керування енергоспоживанням, що дозволяє ефективно регулювати витрати електроенергії в залежності від навантаження мережі. Такі функції, як автоматичне вимикання портів у режимі очікування, сприяють зменшенню споживання електроенергії в періоди низької активності мережі.

У результаті аналізу функціональних особливостей комутатора Cisco C9300-48P-E встановлено, що даний мережевий пристрій є високопродуктивним та ефективним рішенням для сучасних корпоративних мереж. Наявність 48 портів і високою пропускною здатністю, забезпечується потужність у великих мереж. Інтеграція технології PoE розширює сферу його застосування, зокрема в офісах, де необхідне живлення для різних пристроїв, таких як IP-камери та телефони. Захист мережі реалізується завдяки використанню стандартів та механізмів захисту. Адаптивна розширюваність та енергоефективність завдяки інтелектуальному керуванню енергоспоживанням роблять комутатор гнучким та придатним для використання в різних сценаріях. Його сумісність зі стандартами та інтеграція з іншими продуктами Cisco роблять комутатор C9300-48P-E частиною мережевої інфраструктури, що сприяє високій ефективності та управління.

Література

1. Cisco. (Офіційний веб-сайт Cisco) [Електронний ресурс]. – Доступний з https://www.cisco.com/

2. Cisco Catalyst 9300 Series Switches Data Sheet: [Електронний ресурс]. – Доступний з https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.html

3. Awasthi, Anshuman. (2020). Network Classification for an Enterprise. International Journal of Science and Research (IJSR). 9. 635-637. 10.21275/SR20210035306.

4. Alharbi, Hatem & El-Gorashi, Taisir & Elmirghani, Jaafar. (2020). Energy Efficient Virtual Machines Placement over Cloud-Fog Network Architecture.

5. Герговський О., Бурак Н.Є. Аналіз функціональних особливостей комутаторів Layer 2 та Layer 3. Інформаційна безпека та інформаційні технології ІБІТ-2022: збірних тез доповідей IV Міжнародної науково-практичної конференції, 30 листопада 2022 року. – Львів, ЛДУ БЖД, 2022. – С.199-201

УДК 004.42

ВИКОРИСТАННЯ DATA ANALYTICS В ОСВІТНЬОМУ ПРОЦЕСІ SMART-УНІВЕРСИТЕТУ

Придатко О.В. Фігура Л.І.
Львівський державний університет безпеки життєдіяльності, м. Львів

Впровадження Data Analytics в освітньому процесі Smart-університету. Досліджуються збір та аналіз даних, персоналізоване навчання, покращення якості освіти та ефективність викладачів тощо. Робиться акцент на можливостях вдосконалення освіти за допомогою аналітики.

Ключові слова: Data Analytics, студенти, викладачі, персоналізоване навчання.

Implementation of Data Analytics in the educational process of a Smart University. Data collection and analysis, personalized learning, improving the quality of education and teacher effectiveness, etc. are explored. The author emphasizes the possibilities of improving education with the help of analytics.

Keywords: Data Analytics, students, teachers, personalized learning.

Data Analytics – це процес збору, аналізу та використання даних для прийняття рішень та вдосконалення процесів. Важливість Data Analytics в освіті полягає в наступному:

Персоналізоване навчання: Аналітика дозволяє створити персоналізовані навчальні програми для кожного студента, враховуючи їхні потреби та можливості.

Покращення якості навчання: За допомогою аналізу можна вчасно виявити та виправити проблеми в навчальному процесі та покращити якість навчання.

Прогнозування успішності: Data Analytics дозволяє прогнозувати успішність студентів та надавати їм додаткову підтримку, якщо це необхідно.

Ефективність викладачів: Аналітика може допомогти оцінити ефективність викладачів та вчителів, щоб забезпечити найкращу якість навчання.

Типи даних, які можуть бути зібрані в освітньому процесі:

Оцінки студентів: Це включає в себе інформацію про академічні досягнення студентів, такі як оцінки за курси, результати екзаменів, індивідуальні завдання тощо.

Активність на платформі навчання: Інформація про те, як студенти взаємодіють з онлайн-платформами, включаючи час, який вони витрачають на виконання завдань, відвідуваність лекцій та інші онлайн-дії.

Відгуки студентів: Відгуки, скарги або пропозиції, які студенти подають щодо курсів, викладачів або якості освіти.

Біометричні дані: В деяких випадках можуть бути використані біометричні дані, такі як відбитки пальців або розпізнавання обличчя для забезпечення безпеки та ідентифікації студентів.

Анкети та опитування: Дані, зібрані за допомогою анкет та опитувань, можуть допомогти зрозуміти думку студентів про навчання та інші аспекти університетського життя.

У міру просування університетів у цифрову епоху аналітика великих даних використовується для кращого виявлення прогалин у навчанні студентів і надання більш ефективної підтримки. Використовуючи аналітику великих даних, викладачі можуть використовувати статистику на основі даних, щоб точніше визначити сфери, де студентам може знадобитися додаткова підтримка та індивідуальне навчання.

Збираючи дані з оцінювання та повсякденної діяльності, викладачі можуть отримати набагато повніше уявлення про прогрес у навчанні кожного студента. Ці дані можна використовувати для оцінки не лише поточного рівня розуміння студента, але й конкретних сфер, де їм потрібна додаткова допомога. Краще розуміючи індивідуальні потреби кожного, педагоги можуть надати цілеспрямовану підтримку, яка адаптована до рівня розуміння студента.

Аналітику великих даних також можна використовувати для відстеження ефективності навчальних практик. Відстежуючи прогрес студентів, які отримують додаткову підтримку, викладачі можуть визначити, які методи навчання найкраще допомагають їм зрозуміти певний предмет чи концепцію. Ця інформація може бути використана для формування майбутніх навчальних стратегій і забезпечення того, щоб студенти отримували найефективніші інструкції.

Використовуючи аналітику великих даних, викладачі можуть отримати цінну інформацію про прогалини в навчанні студентів, які можуть допомогти підтримати та покращити успішність студентів. Використовуючи інформацію, що керується даними, викладачі можуть переконатися, що студенти отримують індивідуальні інструкції, необхідні для повної реалізації свого потенціалу.

Аналітику даних також можна використовувати для аналізу поведінки студентів і виявлення будь-яких основних проблем, які можуть вплинути на їх навчання. Відстежуючи, як студенти взаємодіють з навчальними матеріалами, університети можуть визначити будь-які моделі поведінки чи вподобання, які можуть вплинути на їхній прогрес. Потім це можна використовувати для прийняття рішень щодо розробки навчального плану та навчання, а також для кращого розуміння того, як студенти навчаються.

Із зростаючим попитом на прийняття рішень на основі даних в освіті Data Analytics відіграє все більш важливу роль у допомозі студентським округам, політикам та іншим зацікавленим сторонам краще зрозуміти осві-

тній ландшафт. Використовуючи потужні інструменти аналізу даних, навчальні заклади можуть отримати цінну інформацію про успішність студентів, ефективність навчальної програми, інвестиції в освіту тощо.

Нещодавні досягнення в аналітиці великих даних спростили для навчальних закладів доступ, аналіз і візуалізацію великих обсягів даних. За допомогою складних методів візуалізації даних навчальні заклади можуть швидко визначати закономірності та тенденції зі своїх даних, які можуть бути корисними для прийняття рішень. Візуалізація даних у такий спосіб може допомогти викладачам визначити сфери можливостей і потенційні сфери вдосконалення, допомагаючи їм приймати більш обґрунтовані рішення.

Методи візуалізації даних також можуть допомогти викладачам визначити кореляції між різними наборами даних, дозволяючи їм знаходити значущу інформацію про успішність студентів та інвестиції в освіту. Наприклад, візуалізацію даних можна використовувати для порівняння успішності студентів у різних університетах або для визначення сфер можливостей для вдосконалення навчальної програми. Це може допомогти поінформувати осіб, які приймають рішення, про те, які інвестиції слід зробити для досягнення максимального ефекту.

Data Analytics також надає навчальним закладам можливість відстежувати та аналізувати прогрес студентів з часом. Використовуючи прогнозну аналітику та алгоритми машинного навчання, навчальні заклади можуть отримати уявлення про моделі навчання студентів і визначити сфери, де студентам може знадобитися додаткова підтримка. Потім ці дані можуть бути використані для інформування про навчальні програми, щоб краще відповідати потребам окремих студентів.

Поєднуючи потужну аналітику з методами візуалізації даних, навчальні заклади можуть скористатися перевагами аналітики Data Analytics для прийняття більш обґрунтованих рішень. Оскільки технології все більше інтегруються в освіту, постійно зростає потреба в розробці персоналізованих стратегій навчання, які максимізують навчальний потенціал кожного студента. Аналітика великих даних надає унікальну можливість досягти цієї мети. Застосовуючи складні методи аналізу даних до великих наборів освітньої інформації, викладачі можуть розробляти стратегії, які визначають сильні та слабкі сторони кожного студента, а також їхні індивідуальні вподобання у навчанні.

Аналітика великих даних використовується для створення детальних профілів індивідуального стилю навчання кожного студента. Завдяки аналізу таких даних, як успішність, поведінка, інтереси й уподобання студентів, викладачі можуть скласти повну картину звичок кожного студента до навчання. Потім ці дані можна використовувати для створення персоналізованих стратегій навчання, адаптованих до індивідуальних потреб і вподобань студента. Ці дані також можна використовувати для виявлення та усунення будь-яких потенційних прогалин або недоліків у навчанні, які можуть існувати.

Аналітику великих даних також можна використовувати для розробки цільових втручань для підвищення залученості та мотивації студентів. Аналізуючи дані студентів, викладачі можуть розробити персоналізовані

стратегії для підтримки індивідуальних навчальних потреб і вподобань студентів. Це допомагає переконатися, що студенти залишаються залученими та мотивованими до навчання.

Використання аналітики великих даних революціонізує підхід викладачів до персоналізованих стратегій навчання.

Data Analytics надає багато можливостей та варіанцій для свого використання, які можна використати та налаштувати відповідно до індивідуальних потреб кожного бажаючого. Це надає можливість розвиватись, вдосконалювати навчання в закладі вищої освіти та пропонувати і впроваджувати інноваційні підходи щодо вдосконалення освітнього процесу.

Література

1. Anderson, C. A., & Dron, J. (2011). Three generations of distance education pedagogy. The International Review of Research in Open and Distributed Learning, 12(3), 80-97.

2. Siemens, G., & Long, P. (2011). Penetrating the Fog: Analytics in Learning and Education. EDUCAUSE Review, 46(5), 30-40.

3. Joksimović, S., Gašević, D., Kovanović, V., Riecke, J., & Hatala, M. (2015). Social presence in online discussions as a process predictor of academic performance. Journal of Computer Assisted Learning, 31(6), 638-654.

4. Siemens, G., & Baker, R. S. (2012). Learning analytics and educational data mining: Towards communication and collaboration. In Proceedings of the 2nd International Conference on Learning Analytics and Knowledge (LAK'12) (pp. 252-254).

5. Arnold, K. E., & Pistilli, M. D. (2012). Course signals at Purdue: Using learning analytics to increase student success. In Proceedings of the 2nd International Conference on Learning Analytics and Knowledge (LAK'12) (pp. 267-270).

6. West, D. M. (2012). Big data for education: Data mining, data analytics, and web dashboards. Governance Studies at Brookings, 4, 1-12.

7. Lynch, C. (2011). Big data: How do your data grow? Nature, 455(7209), 28-29.

8. Baker, R. S., & Siemens, G. (2014). Educational data mining and learning analytics. In Sawyer, K. (Ed.), The Cambridge Handbook of the Learning Sciences (pp. 253-272). Cambridge University Press.

9. Shum, S. B., Ferguson, R., & Martinez-Maldonado, R. (2017). Learning Analytics in Higher Education: Current Innovations, Future Potential, and Practical Applications. Handbook of Learning Analytics (pp. 3-27). SOLAR.

10. Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). Big data: The next frontier for innovation, competition, and productivity. McKinsey Global Institute.

УДК 004.896

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОБРОБКИ ТА АНАЛІЗУ ДАНИХ ПРО ЕВАКУАЦІЮ ПІД ЧАС ПРОВЕДЕННЯ АВАРІЙНО-РЯТУВАЛЬНИХ РОБІТ

Райта Діана, Брошко Володимир, Хлевной Олександр
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто ефективність та перспективи застосування штучного інтелекту в аварійно-рятувальних операціях. Підкреслено вплив швидкої обробки даних на дії рятувальних служб в надзвичайних ситуаціях, а також важливість аналізу графічних даних при проведенні аварійно-рятувальних робіт, зокрема, евакуації населення. Наголошено на важливості методів підрахунку натовпу та проаналізовано їхні можливості.

Ключові слова: штучний інтелект, аварійно-рятувальні операції, швидка обробка даних, аналіз графічних даних.

Effectiveness and prospects of applying artificial intelligence in emergency rescue operations have been considered. The impact of rapid data processing on emergency response actions heas been discussed and the importance of analyzing graphical data in identifying hazardous scenarios has been highlighted. The significance of crowd counting methods and their potential have been emphasized.

***Keywords*:** artificial intelligence, emergency rescue operations, rapid data processing, graphical data analysis.

Ефективність дій рятувальних підрозділів в надзвичайних ситуаціях суттєво залежить від швидкості обробки та передачі даних. Статистичні дані про загиблих та постраждалих підтверджує складність своєчасного прийняття рішень про евакуацію з небезпечних зон. На сьогоднішній день відсутні ефективні системи для оперативного підрахунку людей при масовому їх скупченні, що призводить до затримок у зборі та аналізі даних про надзвичайні ситуації та підвищує ризики для тих, хто опинився в таких умовах. Використання безпілотних літальних комплексів підрозділами ДСНС України є позитивним аспектом для проведення розвідки [1], але обробка отриманих даних вимагає оптимізації через застосування «комп'ютерного зору». З цих причин науково-практичною задачею стає обробка графічних даних аеророзвідки в режимі реального часу за допомогою згорткових мереж для кращого управління рятувальними операціями під час ліквідації надзвичайних подій. Інтеграція систем штучного інтелекту, зокрема згорткових нейронних мереж, в процес обробки та аналізу візуальних даних є перспективною складовою розв'язання проблеми швидкого реагування під час надзвичайних ситуацій.

Такі системи можуть не лише швидко отримувати дані відеопотоку, а й самостійно аналізувати графічні зображення для виявлення небезпеки, підрахунку кількості людей на місцях надзвичайних подій та оцінки ступеня загрози. Завдяки цьому, оперативність рятувальних служб може значно зрости [2], а стратегічне планування та координація дій стати більш ефективними.

Використання методів підрахунку натовпу має широке застосування. Це може бути:

— підрахунок людей в місцях масового скупчення у реальному часі з метою моніторингу їх кількості та подальшого прийняття рішень;

— визначення інтенсивності руху на вулицях для ефективного планування розвитку міської інфраструктури [3].

Підрахунок можна використовувати для обліку відвідуваності на виробництві або в навчальних закладах [3, 4]. Для кожної з цих цілей потрібні власні технології підрахунку.

Наразі дослідники умовно розділяють натовп на щільний і розріджений. Якщо багато людей зібралися в одному місці, то ми маємо справу зі щільним натовпом, а коли людей відносно небагато — це розріджений натовп. Якщо підрахунок розрідженого натовпу відносно простий, то аналіз щільного потребує великих зусиль. Існують три типи підрахунків:

1. Монолітний — штучний інтелект навчається на зображеннях зовнішнього вигляду усього тіла людини.

2. Часткове виявлення — штучний інтелект аналізує лише окремі частини тіла людини, наприклад, голову і плечі, та застосовує до них розроблений класифікатор.

3. Порівняння форм — система малює еліпси навколо тіла людини та підраховує їх кількість.

Наприклад, використання згорткових нейронних мереж для аналізу графічних даних, отриманих від дронів або спеціалізованих камер, дозволяє в реальному часі визначати рух людей, їхні маршрути та поведінку в умовах надзвичайних ситуацій. Такі технології стають критичним інструментом для оперативного реагування під час природних катастроф, аварій, а також допомагають у швидкому прийнятті рішень з евакуації та наданні допомоги потерпілим.

У зв'язку зі стрімким розвитком технологій штучного інтелекту, у перспективі, можливе створення автоматизованих систем, які не лише аналізують графічні дані, але й надають рекомендації та стратегічні вказівки для оптимальних дій під час надзвичайних ситуацій. Такий напрямок досліджень і розробок відкриває широкі можливості для підвищення ефективності та безпеки аварійно-рятувальних операцій в майбутньому.

Література:

1. Хлевной О. В. Нормування вимог пожежної безпеки до евакуаційних шляхів і виходів у закладах середньої освіти з інклюзивним навчанням: дис. ... канд. техн. наук: 21.06.02 / Львів, 2021. – 188 с

2. Гаврись А. П., Хлевной О. В. Software-based method of determining the necessary population evacuation zone in case of a chemical accident. Збірник наукових праць Черкаського інституту пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України «Надзвичайні ситуації: попередження та ліквідація». – Черкаси. – 2022. – 6 (2). – с. 116-128.

3. Зачко О.Б., Головатий О.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. Khlevnoi, O.: Standardization of fire safety requirements for evacuation routes and exits in secondary education institutions with inclusive education. Ph.D. thesis, Lviv State University of Life Safety (2021)

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПЛАНУВАННЯ СТВОРЕННЯ ДОБРОВІЛЬНИХ РЯТУВАЛЬНИХ ФОРМУВАНЬ ДЛЯ СІЛЬСЬКИХ ГРОМАД

Ратушний Андрій, Коваль Назар, Коваль Лілія, Тригуба Богдан
Львівський державний університет безпеки життєдіяльності,
Львівський національний університет природокористування

Виконано аналіз стану застосування інформаційних технологій у процесі створення добровільних рятувальних формувань для сільських громад. Подано головні складові, які впливають на ефективність процесу. Сформульовано задачі та означено сучасні інформаційні технології для підвищення ефективності процесу планування створення добровільних рятувальних формувань.

Ключові слова: інформаційні технології, планування, безпека, сільські громади

An analysis of the state of the application of information technologies in the process of creating voluntary rescue formations for rural communities was performed. The main components that affect the efficiency of the process are presented. Tasks were formulated and modern information technologies were defined to increase the efficiency of the planning process of creating voluntary rescue formations.

Keywords: information technologies, planning, security, rural communities

Сьогодні інформаційні технології стають необхідною складовою для розвитку та управління різноманітними аспектами життя та діяльності на території громад. Однією із актуальних предметних галузей застосування цих технологій є процеси планування та створення добровільних рятувальних формувань для сільських громад. При цьому існують свої специфічні особливості виконання зазначених процесів, так як у сільській місцевості безпекові процеси нехтуються, що не забезпечує належний захист населення від різноманітних викликів, таких як природні катастрофи, аварії та інші надзвичайні ситуації та події. У цьому контексті ефективне планування та організація проведення заходів із ліквідації надзвичайних ситуацій та подій значною мірою залежить від наявності та використання сучасних інформаційних технологій.

Застосування інформаційних технологій у процесі створення добровільних рятувальних формувань для сільських громад відкриває нові можливості для ефективного реагування на надзвичайний стан та забезпечення безпеки життя та майна населення. Враховуючи швидкі темпи технологічного розвитку, необхідно активно впроваджувати інноваційні рішення для оптимізації процесів планування, координації та взаємодії рятівників.

Виконаємо аналіз головних складових, які впливають на ефективність процесу планування створення добровільних рятувальних формувань для сільських громад (рис. 1).

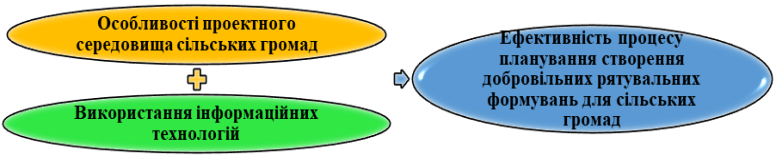


Рисунок 1 – Головні складові, які впливають на ефективність процесу планування створення добровільних рятувальних формувань для сільських громад

Особливості проектного середовища сільських громад можуть впливати на ефективність процесу планування створення добровільних рятувальних формувань. Зокрема, це стосується рівня ризику надзвичайних ситуацій, розміру громади, економічної ситуації, соціально-культурних складових. Щоб підвищити ефективність процесу планування створення добровільних рятувальних формувань для сільських громад, необхідно враховувати особливості проектного середовища цих громад. Інформаційні технології (ІТ) використовуються для підвищення ефективності процесу планування створення добровільних рятувальних формувань для сільських громад. Це стосується процесів збору та аналізу інформації, поширення інформації, управління процесом планування, а також організації навчання та підготовки рятувальників. Використання ІТ може значно підвищити ефективність процесу планування створення добровільних рятувальних формувань для сільських громад. Це допоможе забезпечити створення більшу ефективність діяльності формувань, які будуть здатні швидко та результативно виконувати роботи із ліквідації надзвичайних ситуацій.

Наше дослідження стосується аналізу та обґрунтування доцільності використання сучасних інформаційних технологій для реалізації процесів планування та створення добровільних рятувальних форм для сільських громад. Ініціація та формулювання окремих задач із впровадженням сучасних інформаційних технологій у практику створення добровільних рятувальних формувань в сільських регіонах, є основою для окреслення перспектив розвитку цього напряму та розроблення відповідного інструментарію (табл. 1).

Таблиця 1 – Задачі та сучасні інформаційні технології для підвищення ефективності процесу планування створення добровільних рятувальних формувань

Задача	Сучасні інформаційні технології для їх вирішення	Переваги використання інформаційних технологій
Прогнозування стану безпеки об'єктів на території сільських громад	Машинне навчання	Аналіз великих даних для встановлення закономірностей та трендів у безпеці. Можливість автоматизації процесу прогнозування та попередження можливих небезпек. Покращення точності та об'єктивності прогнозів.
Ефективне планування рятувальних заходів	Географічні інформаційні системи (ГІС), дрони для аерофотозйомки, інструментарій аналізу даних	Покращення точності та швидкості планування заходів у надзвичайних ситуаціях. Забезпечення зручності взаємодії рятівників та координації їхніх дій.
Швидка передача інформації під час надзвичайних подій та ситуацій	Сучасні інформаційні системи екстреної комунікації, відеоконференції	Забезпечення оперативного обміну інформацією між рятівниками та керівництвом. Можливість віддаленого координації заходів під час надзвичайних ситуацій.
Системи моніторингу стану інфраструктури сільських територій	Інтернет речей (IoT), сенсорні мережі	Системний моніторинг стану інфраструктури для оперативного виявлення та усунення проблем. Можливість передбачення можливих ризиків та покращення управління інфраструктурою.

Висвітлення сучасних тенденцій та інновацій у сфері інформаційних технологій для захисту населення сільських громадах є основою для подальших досліджень у напрямку підвищення рівня безпеки сільських територій до виникнення надзвичайних ситуацій та подій, а також збереження майна та зниження можливих збитків.

Література

1. Ratushny R., Tryhuba A., Bashynsky O., Ptashnyk V. Development and usage of a computer model of evaluating the scenarios of projects for the creation of fire fighting systems of rural communities. *XI-th International Scientific and Practical Conference on Electronics (ELIT-2019).* 2019. P. 34-39.

2. Tryhuba A., Ratushny R., Bashynsky O., Shcherbachenko O. Identification of firefighting system configuration of rural settlements. *Fire and Enviromnental Safety Engineering. MATEC Web Conf*. FESE 2018. 247.

3. Martyn Y., Smotr O., Burak N., Prydatko O., Malets I. Software for Shelter's Fire Safety and Comfort Levels Evaluation. In book: Data Stream Mining & Processing. 2020. pp.457-469.

УДК378.147:372.881.111.1

ЕФЕКТИВНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ВИКЛАДАННІ АНГЛІЙСЬКОЇ МОВИ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Ремез Інна, Шихненко Катерина
Інститут державного управління та наукових досліджень з цивільного захисту, м. Київ

Анотація. Інформаційні технології сприяють осучасненню викладачами освітнього процесу, забезпечують ефективність навчання та постійний зв'язок між викладачами та слухачами в умовах змішаного та дистанційного навчання. Метою діяльності викладача є мотивація слухачів до вивчення англійської мови через використання цифрових додатків та платформ.

Ключові слова: інформаційні технології, навчання англійської мови, навчальні платформи та додатки, дистанційне та змішане навчання.

Abstract. Information technologies help teachers to modernize the process of learning, ensure the effectiveness of the educational process and provide constant communication between students and teachers in the conditions of mixed and distance learning. Using information technologies contribute to the motivation of students in learning English. The teacher's goal is to motivate students to learn English using digital platforms and apps.

Keywords*:* information technology, English language learning, educational platforms and applications, distance and blended learning.

Актуальність теми полягає в тому, що в умовах роботи викладача закладу вищої освіти в форматах дистанційного та змішаного навчання в Україні постає необхідність переспрямування процесу викладання англійської мови на використання сучасних електронних ресурсів та засобів.

Серед навчальних можливостей слухачів (студентів) мають бути електронні словники, додатки для мобільних пристроїв, системи машинного перекладу та платформи для дистанційного навчання, що розширюють освітній потенціал і сприяють розвитку навчальних здібностей слухачів (студентів). Тому ефективне використання інформаційних технологій у процесі викладання та навчання англійської мови відповідає найважливішим потребам сьогодення.

Пропонуємо для розгляду окремі платформи і ресурси, створені задля допомоги викладачам, що можуть осучаснити навчання слухачів (студентів), сприяють соціальній взаємодії в умовах дистанційного та змішаного навчання. Нижче наведено сучасні цифрові інструменти для викладання англійської мови та рекомендації щодо форм та методів роботи з ними для стимулювання навчальної діяльності слухачів та розвитку їх пізнавальних інтересів.

Сервіси на основі штучного інтелекту (ШІ) реалізують такі можливості, як розпізнавання мовлення, що забезпечує рівний доступ до навчання слухачам з обмеженими можливостями, слухачам (студентам) з іншомовного середовища та викладачам, що бажають отримати користь від більшої адаптивності та персоналізації цифрових інструментів для навчання. Штучний інтелект може допомогти розробити або вдосконалити заняття, а також налагодити процес пошуку, добору та адаптації матеріалу для використання в освітньому процесі.

Цифровий сторітелінг застосовується для того, щоб оживити розповідь: відображення даних, створення графічних об'єктів, демонстрація зображень і включення інтерактивних елементів дозволить слухачам (студентам) глибше сприйняти, дослідити та пережити розповідь. Цей метод допоможе адаптувати дослідницьку роботу до цільової аудиторії, результатом якої буде створення мультимедійного есе чи розповіді. Сервіс ESRI Story Maps дозволяє розробити власні карти, додавати тексти та зображення мультимедійного вмісту. Особливо ефективно платформа використовується для створення розповідей про географічні місця та об'єкти.

Важливість і доцільність використання подкастів в умовах відсутності іншомовного середовища визнані багатьма науковцями. Зокрема А. Міддлтон (A. Middleton) зазначає їх доступність та зручність у використанні, оскільки під час роботи з ними немає обмежень у часі та просторі [3]. Завдання, створені з опорою на подкасти, характеризуються гнучкістю, незалежністю від пристроїв, мобільністю та керованістю користувачем.

Цифрова платформа Adobe Spark (Spark Pages) використовується для коротких, лінійних історій, які мають багато візуальних елементів. Цю платформу доцільно застосовувати для розвитку навичок говоріння та цифрових навичок. Доступ до галереї зображень допоможе оживити розповідь. Сервіс використовується для створення невеликих візуальних проектів.

eFront є однією з навчальних платформ з необмеженим функціональними можливостями. Система eFront створена для управління та підтримки навчання. Завдяки потужним параметрам налаштування у eFront можливо створити навчальну платформу, що не схожа на жодну іншу.

MangaChat – це платформа на зразок щоденника у вигляді коміксів, яка допомагає викладачам запроваджувати навчання слухачів та студентів через соціально-емоційний аспект, як в закладі освіти так і під час самостійної роботи вдома. Через ведення щоденника та обміну письмовими та усними повідомленнями платформа сприяє розвитку навичок письма та комунікативних навичок, особливо корисна для слухачів (студентів) перших курсів, які адаптуються до нового студентського життя.

Навчання впродовж життя має стати життєвою необхідністю для кожного учасника навчального процесу. Провайдер масових відкритих онлайн-курсів (MOOC) edX співпрацює з провідними університетами світу

та пропонує високоякісні онлайн-курси для здобувачів вищої освіти у всьому світі, надає широкий вибір курсів для підвищення кваліфікації викладачів та здобуття нових знань для слухачів та студентів.

Для полегшення процесу перекладу з однієї мови на іншу створено спеціальні онлайн словники з визначеними парами мов. Американський мовознавець С. Лендау акцентує на значному впливі комп'ютерних технологій на сучасну лексикографію [1]. Переваги, які має онлайн-словник для вивчення англійської мови над друкованим, це – доступність, постійне оновлення інформації, спрощений пошук та мультимедійний контент.

The Longman Dictionary of Contemporary English Online здійснює пошук з контролем правопису, визначень, можливих словосполучень зі словами, надає велику кількість прикладів і малюнків. Перевагою даного словника є те, що визначення в ньому подаються простою мовою, що полегшує не носіям мови розуміння значення слів, оскільки в словнику не передбачений переклад.

Cambidge Online є цифровою версією Кембриджського словника. Ресурс має зручне меню з можливістю обрати категорію – переклад, визначення, американську англійську мову, фразові дієслова та ідіоми. Також, у словнику представлені англійський та американський варіанти вимови слів.

Гейміфікація освітнього процесу сприяє формуванню позитивної мотивації слухачів (студентів) до оволодіння навчальним матеріалом. Як приклад, наведемо Kahoot, що є інтерактивною цифровою навчальною платформою як для використання в дистанційному навчанні, так і для навчання в аудиторії в ігровій формі. Завдання у формі вікторин є дієвим інструментом перевірки знань слухачів (студентів).

Використання різноманітних цифрових засобів та платформ, згаданих вище, є ефективним засобом для розробки та удосконалення онлайн-занять, а також для створення презентацій, цифрових розповідей тощо. Використання інформаційних технологій відкриває нові можливості як для здобувачів освіти, так і для викладачів.

Література

1. Лендау С. І. Словники: мистецтво та ремесло лексикографії. Київ: К.І.С., 2012.

2. How to Use Technology Effectively to Transform Your ESL Classroom. FluentU English Educator Blog. URL: https://www.fluentu.com/blog/ educatorenglish/ esl-technology-2

3. Middleton A. 100 great ideas for educational podcasting. Sheffield Hallam University, 2008. URL: http://teaching.shu.ac.uk/podcast/pdf/edpodworkbook.pdf.

4. Modern Ways to Use Technology in ESL Instruction. Busy Teacher: web-site. URL: https:// busyteacher.org/13732-using-technology-eslinstruction-10-modern-ways.html.

УДК 004.93'1, 004.89

АНАЛІЗ МОЖЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ ТА ПОДАЛЬШОГО ГУМАНІТАРНОГО РОЗМІНУВАННЯ

Рибалка Анастасія, Скорлупін Олександр, Подорожняк Андрій
Національний технічний університет
«Харківський політехнічний інститут», м. Харків

Інтенсивне впровадження новітніх технологій штучного інтелекту, великі перспективи застосування різноманітних роботизованих безпілотних систем, використання різноманітних засобів дистанційного зондування та сучасних алгоритмів обробки сигналів та зображень є передумовами вирішення проблеми виявлення вибухонебезпечних предметів та подальшого гуманітарного розмінування забрудненої мінами й боєприпасами, що не розірвалися території України. У доповіді проведено аналіз актуальних сучасних та перспективних технологій робототехніки і штучного інтелекту, що дозволять пришвидшити та забезпечити процес майбутнього виявлення вибухонебезпечних предметів і подальшого гуманітарного розмінування.

Ключові слова: штучний інтелект, роботизована безпілотна система, виявлення вибухонебезпечних предметів, розмінування

Intensive implementation of the latest artificial intelligence technologies, great prospects for the use of various robotic unmanned systems, the use of various remote sensing tools and modern signal and image processing algorithms are prerequisites for solving the problem of detecting explosive objects and further humanitarian demining of the territory of Ukraine contaminated by mines and unexploded ammunition. The report analyzes current modern and promising technologies of robotics and artificial intelligence, which will allow speeding up and ensuring the process of future detection of explosive objects and further humanitarian demining.

Key words: artificial intelligence, robotic unmanned system, detection of explosive objects, demining

Із початком війни та повномасштабної агресії росії проблема розмінування стала як ніколи актуальною. За попередньою оцінкою наразі близько 30% території України забруднено мінами й боєприпасами, що не розірвалися, артилерійськими снарядами й іншими смертоносними побічними продуктами війни. За інформацією Мінекономіки, з початку 2023 року в Україні під час очищення від мін обстежили понад 225 тисяч гектарів земель сільськогосподарського призначення. [1, 2].

Із 24 лютого 2022 року до 30 червня 2023 року Управління Верховного комісара ООН з прав людини зафіксувало 905 випадків загибелі або поранення цивільних осіб внаслідок мінних інцидентів і поводження з вибухонебезпечними залишками війни: 293 загиблих і 612 поранених [3].

Результати практичних випробувань та наукових досліджень вказують на те, що продуктивність одного сапера у процесі очищення території від вибухонебезпечних об'єктів становить від 15 до 25 квадратних метрів на день, залежно від рельєфу місцевості та концентрації вибухівки [4]. Тому терміни розмінування всієї території України можна буде спрогнозувати лише після закінчення бойових дій і нажаль може зайняти багато років. Іноді гуманітарне розмінування називають процесом після війни. Однак, у нас немає стільки часу на це враховуючи безпрецедентні розміри площ, які забруднені вибухівкою та зброєю.

Саме це підкреслює важливість розробки нових технологій зі штучним інтелектом у сфері розмінування. Штучний інтелект в контексті протимінної системи – це технологічна система, яка використовує різноманітні сенсори, аналіз даних і алгоритми машинного навчання для виявлення та нейтралізації вибухових пристроїв або нерозірваних вибухових речовин на території, що потенційно небезпечна для людей. Протимінні системи, побудовані на базі штучного інтелекту, можуть забезпечити значно вищу продуктивність та ефективність у процесі очищення великих територій від потенційно небезпечних об'єктів. Їхні можливості адаптації до різних умов, відсутність фізичної втоми та висока точність роботи роблять їх незамінними помічниками у розмінування територій, де безпека та ефективність є важливими пріоритетами.

Метою доповіді є аналіз технологій робототехніки та штучного інтелекту, що дозволять пришвидшити та забезпечити процес майбутнього виявлення вибухонебезпечних предметів і подальшого гуманітарного розмінування.

Застосування протимінних систем зі штучним інтелектом може сприяти швидкому відновленню територій і зменшенню ризику для життя та здоров'я людей, які займаються розмінуванням. Ця технологія може значно підвищити безпеку, результативність та продуктивність процесу розмінування, сприяючи загальному поліпшенню ситуації та життєвих умов на території України.

Основним винаходом останнього десятиліття став георадар, що закріплюється на металодетекторі. Але складний та дорогий пристрій тільки починає переходити з рук військових до державної служби України з надзвичайних ситуацій і має ті ж обмеження, що у металодетекторів – він може давати неправдиві свідчення, і з його підтримкою оператор не здатний визначити, який саме об'єкт він знайшов [5]. Також існують спроби оснастити безпілотні робототехнічні платформи термографічними та мультиспектральними камерами, які будуть здатні виявляти міни в землі [6]. Дрони можуть перетворюватися на літаючі металодетектори, оснащені георадаром. Однак по мінному полю може здійснювати подорож і саморухливий робототехнічний пристрій, який буде занадто легкий для того щоб не здетонувати міни, і тоді сапер буде на безпечній відстані навіть якщо це станеться.

Керуючись чинним Законом України «Про протимінну діяльність в Україні», а також враховуючи положення статуту «Міжрегіонального центру гуманітарного розмінування», виокремлено важливість реалізації комплексу заходів, спрямованих на усунення небезпек, що пов'язані з наявністю вибухонебезпечних об'єктів. Ці заходи включають проведення нетехнічного та технічного обстеження територій, складання карт, виявлення, безпечне усунення або знищення вибухонебезпечних предметів. У зв'язку з поточною ситуацією в країні, де введений воєнний стан та загострена економічна ситуація, Україні обмежена засобами, необхідними для проведення таких нагальних заходів.

Проведений аналіз показав, що найбільш перспективним може бути застосування технологій штучного інтелекту та робототехнічних систем на базі безпілотних авіаційних та надлегких наземних роботизованих засобів. Така система може мати можливість виявляти та розрізняти міни, снаряди та інші вибухові пристрої. Вона буде базуватися на високо розвинутих алгоритмах обробки зображень, сигналів та даних, які допоможуть ідентифікувати потенційні загрози а також впевнено та безпечно виявляти і розмінувати вибухові пристрої на мінному полі або в зоні конфлікту.

Література

1. Тютюненко, Н. Як будуть розміновувати Україну: важливі деталі від заступника міністра економіки, 31.10.2023 [Електрон. ресурс]. – Режим доступу: https://telegraf.com.ua/ukr/ukraina/2023-10-31/5815328-yak-budut-rozminovuvati-ukrainu-tsikavi-detali-vid-zastupnika-ministra-ekonomiki.

2. Heslop P. UNDP trials innovative technologies that could rid Ukraine of landmines in 10 years, 11.10.2023 [Електрон. ресурс]. – Режим доступу: https://english.nv.ua/nation/undp-trials-innovative-technologies-that-could-rid-ukraine-of-landmines-in-10-years-50359743.html

3. Втрати серед цивільних осіб в Україні у період з 24 лютого 2022 року до 30 червня 2023 року. Моніторингова місія ООН з прав людини в Україні, 07.07.2023 [Електрон. ресурс]. – Режим доступу: https://ukraine.un.org/sites/default/files/2023-07/Civiliancasualtiesin20Ukraine20June%20202320UKR.pdf

4. Стандартна операційна процедура 09.11/ДСНС. Порядок проведення органами та підрозділами цивільного захисту очищення (розмінування) району ведення бойових дій. Затверджено: Головою ДСНС 04.03.2020, 76 с. [Електрон. ресурс]. – Режим доступу: https://dsns.gov.ua/upload/2/6/8/9/6/5/EvgyR9W0tBTYzldCjhjd5i5wlPhiSNqzwQEaeJ0y.pdf

5. Fedorenko, G. Robotic-biological systems for detection and identification of explosive ordnance: concept, general structure, and models / H. Fesenko, V. Kharchenko, I. Kliushnikov, I. Tolkunov // Radioelectronic and Computer Systems. – 2023. – 2(106). – P. 143–159. https://doi.org/10.32620/REKS.2023.2.12

6. Подорожняк, А. О. Метод інтелектуальної обробки мультиспектральних зображень / А. О. Подорожняк, Н. Ю. Любченко, О. Д. Лагода // Системи обробки інформації. – 2015. – Вип. 10 (135). – С. 123-125. [Електрон. ресурс]. – Режим доступу: https://www.hups.mil.gov.ua/periodic-app/article/13413/soi_2015_10_28.pdf

УДК 81`243:[378.147:004.9]

ФОРМУВАННЯ ІНШОМОВНОЇ КОМУНІКАТИВНОЇ КОМПЕТЕНТНОСТІ СЛУХАЧІВ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ ЗІ СПЕЦІАЛЬНИМИ ЗІ СПЕЦІАЛЬНИМИ УМОВАМИ НАВЧАННЯ ЗАСОБАМИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЇЙ

Романюк Вікторія
Інститут державного управління та наукових досліджень з цивільного захисту

Анотація. Розглянуто проблему формування іншомовної комунікативної компетентності у закладах зі спеціальними умовами навчання за допомогою інформаційних технологій. Визначено проблеми, що є актуальними для закладів зі спеціальними умовами навчання. Наведено ресурси, які потрібно використовувати у процесі формування іншомовної комунікативної компетентності: вже готові платформи, онлайн-ресурси та інтерактивні методи навчання, які сприяють вивченню іноземної мови.

Ключові слова: іншомовна підготовка, інформаційно-комунікативні технології, навчальний процес, онлайн-ресурси, інтерактивні методи навчання.

Annotation. The problem of formation of foreign language communicative competence in institutions with special educational conditions with the help of information technologies is considered. The problems that are relevant for institutions with special educational conditions have been identified. The resources that should be used in the process of forming foreign language communicative competence are presented: ready-made platforms, online resources and interactive teaching methods that contribute to learning a foreign language.

Keywords: foreign language training, information and communication technologies, educational process, online resources, interactive learning methods.

Іншомовна підготовка слухачів вищих навчальних закладів зі спеціальними умовами навчання набуває особливого значення в реаліях сьогодення. Адже, іншомовна комунікативна компетентність – це здатність здобувачів вищої освіти отримувати необхідну інформацію іноземною мовою для подальшого використання у професійній діяльності та під час виконання службових обов'язків.

Для закладів зі спеціальними умовами навчання є актуальними такі проблеми: 1. Неоднорідність навчальних груп: за віком; рівнем іншомовної підготовки курсантів; життєвим досвідом − у групі як випускники загальноосвітніх шкіл, так і військовослужбовці за контрактом. 2. Особливість навчальних груп військових навчальних закладів: підпорядкованість курсантів вимогам єдиного навчально-виховного процесу; дотримання військової дисципліни та правопорядку; високий ступінь самоуправління; чітка регламентація стосунків і функціональна залежність членів групи, яку визначає система субординації; інтенсивність спілкування членів групи; єдиноначальність у координованій діяльності [3, с. 36].

Використання інформаційних технологій в навчальному процесі у закладах вищої освіти не є новим, але й досі залишається актуальним. Сучасні Інтернет-технології відкривають широкі можливість перед викладачами (для викладання) та здобувачами вищої освіти (для навчання).

Інформаційно-комунікаційні технології – це система сучасних інформаційних методів, прийомів праці і їх організації на основі комп'ютерно-технічних засобів, спрямованих на збирання, зберігання, опрацювання, накопичення, передавання, розповсюдження, представлення й використання інформації, що розширює можливості людини в суспільній діяльності [1].

Інформаційні технології – важливий інструмент поліпшення якості освіти, адже дозволяють необмежено розширити доступ до інформації тощо. Застосування інформаційних технологій повністю змінює роль і місце викладача та здобувача вищої освіти в системі «викладач – інформаційна система – здобувач» [4, с. 454].

Інформаційні технології можна розділити на три групи:

1) ***уже готові платформи для дистанційного навчання:***

Moodle – модульне об'єктно-орієнтоване динамічне навчальне середовище, що забезпечує передачу інформації та оцінювання навчальних досягнень.

Sakai – ресурс для очного, онлайн-навчання та змішаних курсів, де можна розмістити тест, вікторину та завдання.

Lotus Learning Space – платформа, що дає можливість навчатись в асинхронному режимі та брати участь у онлайн заняттях в реальному часі.

2) ***онлайн-ресурси:*** https://wordwall.net/ – онлайн-ресурс має значну кількість матеріалів, серед них різного роду тестові завдання, вправи на відповідність, вікторини тощо. Даючи відповіді на питання, студенти відразу ж отримують відповідь, правильна вона чи ні.

https://www.liveworksheets.com/ – онлайн-ресурс, який можна використовувати як на початку заняття, для актуалізації опорних знань, так і наприкінці заняття, для перевірки засвоєного матеріалу. Адже тут є значна кількість бланків (worksheets) з завданнями різного типу. Студенти заповнюють бланки самостійно та після виконання можуть перевірити свої відповіді.

https://learningapps.org/ – онлайн-ресурс, який має найбільшу кількість завдань: "Знайти слово", "Вгадати слово", "Кросворд", "Вікторина", "Заповнити пропуски", "Знайти пару слову" тощо. Також тут є багато різноманітних країнознавчих розробок, які дозволяють зробити заняття цікавим та інформативним.

https://www.wordclouds.co.uk/ – онлайн-ресурс, який доцільно використовувати для проведення різного роду вікторин, щоб активізувати та закріпити знання. Завдяки цьому ресурсу можна створити так звану "хмару" до якої можна додавати будь-які слова, а також оформити її у вигляді будівлі, дерева, серця тощо.

https://crosswordlabs.com/ – безкоштовний онлайн-ресурс для створення кросвордів. Він найпростіший та найшвидший серед тих, що ми зустрічали для підготовки до занять. Цей ресурс ідеально підходить для етапу автоматизації лексичних одиниць [2].

3) ***інтерактивні методи навчання:***

брейнстормінг – інтерактивний мозковий штурм, призначений для створення креативних ситуацій; *робота в парах* – парі учасників ставиться проблема або питання, що потребують вирішення. Цей вид діяльності дозволяє учасниками формувати та висловлювати свої власні думки; *групові дискусії* – учасники обговорюють одну проблему, знаходячись в різних групах, що мають різне бачення; *аналіз реальних проблем* – аналіз кейсів з реальними проблемами; *сесія «питання-відповідь»* – кожен слухач отримує власне питання на яке потрібно дати письмову відповідь.

Отже, інформаційні технології є дієвим інструментом формування іншомовної комунікативної компетентності. Вони забезпечують суттєве підвищення якості набутих знань, удосконалення мовленнєвих вмінь та навичок, мотивують до навчання, оволодіння іноземною мовою, стимулюють мовно-розумову діяльність та інтерес до індивідуального навчання.

Література

1. Нетьосов С. Використання інформаційно-комунікаційних технологій на уроках правознавства. URL: https://www.researchgate.net/publication/341919990 (дата звернення: 22.11.2023).

2. Романюк В. Л. Застосування онлайн-інструментів на заняттях з англійської мови у процесі формування лінгвосоціокультурної компетентності у майбутніх вчителів англійської мови. URL: http://www.economy-confer.com.ua/full-article/4221/ (дата звернення: 22.11.2023).

3. Романюк В.Л., Лещенко А.В. Інтерактивні методи навчання у формуванні професійної іншомовної комунікативної компетентності майбутніх офіцерів Національної гвардії України в умовах воєнного стану. *Науковий вісник "Київського інституту Національної гвардії України"* № 1(2) 2023. с. 34-41.https://doi.org/10.59226/2786-6920.1.2023.34-41

4. Романюк В.Л. Роль інформаційних технологій у процесі формування іншомовної комунікативної компетентності фахівців сектору безпеки та оборони в умовах воєнного стану. *Актуальність та особливості наукових досліджень в умовах воєнного стану:* матеріали ІІІ Міжнародної науково-практичної інтернет-конференції з нагоди відзначення дня науки -2023 в Україні (23 травня 2023). Київ: ДНДІ МВС України. 2023. с. 454-457.

УДК 681.51

РОЗРОБКА УНІВЕРСАЛЬНОГО ПРИСТРОЮ СПРЯЖЕННЯ АПАРАТУРИ ПЕРЕДАЧІ ДАНИХ З ПЕОМ

Рудаков Сергій, Рудаков Ігор
Національний університет цивільного захисту України,
Національний технічний університитет «ХПІ»

Анотація В роботі надані пропозиції щодо апаратно-програмного спряження апаратуру передачі даних спеціального призначення (АПД СП) з ПЕОМ. Було досліджено інформаційне спряження АПД СП АІ-011 з персональною електронно-обчислювальною машиною (ПЕОМ). Запропонований метод перетворення кодограм з формату обміну інформації в АПД СП АІ-011 до формату інтерфейсу RS-232 послідовного COM-порту (USB-порту) ПЕОМ та зворотно у реальному масштабі часу. Проведено дослідження особливостей обміну інформацією між елементами автоматизованої системи управління та математичного і програмного забезпечення її функціонування.

Ключові слова: апаратура передачі даних спеціального призначення, апаратно-програмне спряження

Proposals for hardware and software conjugation of the special-purpose (SP) data transmission equipment (DTE) AI-011 with a personal electronic computer (PEC). Process of studying the information conjugation of the SP DTE AI-011 with a PEC. The purpose of research is to convert codagrams from the format of information exchange in the DTE SP AI-011 to the format of the RS-232 interface of the serial COM port (USB port) of a computer and vice versa in real time. To study the features of information exchange between the elements of the automated control system and the mathematical and software of its functioning. The expediency of the project implementation is substantiated.

Keywords*:* special-purpose data transmission equipment, hardware and software interfacing.

На даний час спостерігається достатньо суттєве збільшення обсягів інформації, яка циркулює у загальній системі управління засобами військового призначення, що призводить до підвищення вимог щодо якості функціонування підсистем збору і обробки інформації, що отримується. Відомі інтерфейсні карти (ІК), що з'єднують апаратуру передачі даних (АПД) спеціального призначення (СП) АІ-011 з електронним обчислювальним комплексом спеціальних машин військового призначення здійснюють прийом та передачу інформації (інформаційних електричних сигналів) у вигляді формалізованих повідомлень (кодограм і бланків).

Абонентські комплекти АПД СП АІ-011 розміщуються на борту засобів розвідки та АСУ. Вони призначені для захисту переданих даних від перешкод та перетворення даних з метою подальшої передачі їх за стандартними каналами зв'язку. Для підвищення достовірності передавання даних в АПД СП АІ-011 використовується циклічне кодування. Воно дає

змогу за ймовірності спотворення одного біта, що дорівнює 10-2, знизити ймовірність неправильного приймання повідомлення до 10-5.

АПД СП АІ-011 дає змогу вести обмін даними зі швидкостями 600 бод із 6 абонентами. В АСУ 9С470М1 швидкість передавання даних становить 1200 бод. Отже, АПД СП АІ-011 призначена для передачі і прийому спільно із засекреченої апаратури зв'язку (ЗАЗ) закритих секретних даних у реальному масштабі часу по дротяних, радіо, радіорелейних і тропосферних каналах тональної частоти, по телеграфних каналах через ППС-ТТ, по каналах обладнаним апаратурою «Інтер'єр», а також у режимі прийому по каналах, що обладнані також радіостанціями Р-832, Р-862 (Р-863). При роботі із апаратурою ЗАЗ АПД СП АІ-011 забезпечує захист від помилок тільки синхропосилки апаратури ЗАЗ.

Також АПД СП АІ-011 призначена для роботи в рухомих комплексах та виконує функцію захисту даних від помилок і перетворення їх для передавання стандартними телефонними каналами дротових, табельних, радіорелейних і короткохвильових ліній зв'язку. Як дані можлива радіолокаційна інформація, що передана у режимі зі стиранням, та дані команд керування, що вимагають підвищеної ймовірності доведення.

АПД СП АІ-011 забезпечує сполучення з каналом зв'язку і з кінцевим обладнанням за стиками (інтерфейсом) відповідно С1 (ОСТ ГО.208.004) та С2 (ГОСТ 18145-72).

Основні технічні характеристики АПД СП АІ-011:

- швидкість передавання даних – 600, 1200 Бод;
- довжина кодової комбінації – n=69, n=117;
- спосіб захисту від помилок – циклічний код, що утворює поліном Q(x)=x16+x12+x5+1;
- рівень вихідного сигналу – від 0... до -40 дб;
- вид модуляції сигналу – частотна модуляція;
- напруга живлення приладу – 27 В;
- споживана потужність – не більше 75 Вт.

Розроблено і запропоновано УПС АПД СП АІ-011 з ПЕОМ, блок-схема якого наведена на рисунку 1.

До складу УПС входить: мікропроцесор CPU 1 з використанням спеціального програмного забезпечення (СПЗ); мікропроцесор CPU 2 з використанням СПЗ; індикація синхронізації; індикація живлення; індикація прийому інформаційних електричних сигналів з CPU 2; індикація передачі інформаційних електричних сигналів на CPU 2; буферні підсилювачі прийому інформаційних електричних сигналів; буферні підсилювачі передачі інформаційних електричних сигналів; підсилювач прийому-передачі інтерфейсу RS-232; COM-порт; перехідний пристрій з COM-порту на USB-порт.

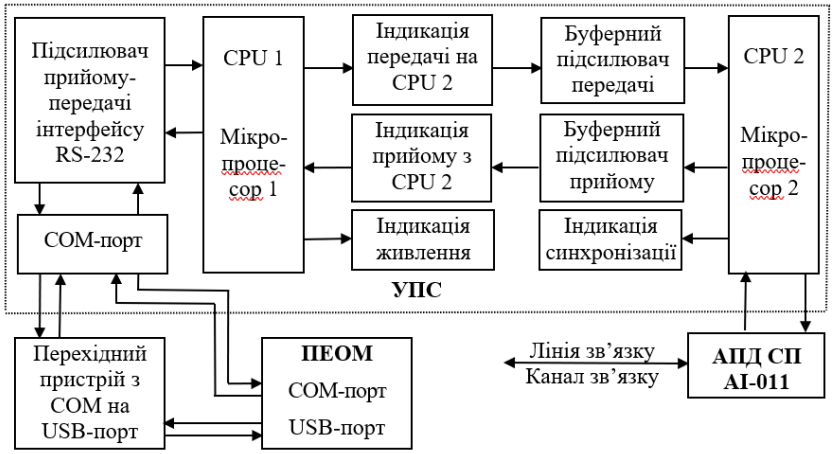


Рисунок 1 – Блок-схема універсального пристрою спряження

Усі функції по організації обміну інформаційними електричними сигналами між універсальним пристрієм спряження (УПС) і ПЕОМ, УПС і АПД СП АІ-011 реалізовані на програмному рівні, що забезпечує передачу даних у симплексному (з адресою і без адреси), попереміннo-симплексному (з адресою і без адреси) та дуплексному режимах роботи.СПЗ мікропроцесору CPU 1 (мікропрограма) реалізує алгоритм перетворення кодограм з формату обміну інформаційними електричними сигналами в АПД СП АІ-011 до формату інтерфейсу RS-232 послідовного COM-порту ПЕОМ та зворотно. За необхідністю обмін інформацією можливо здійснювати також по USB-порту через перехідний пристрій з COM-порту на USB-порт.

Таким чином, розроблено СПЗ для мікропроцесору УПС, яке реалізує алгоритм перетворення кодограм з формату обміну інформаційними електричними сигналами в АПД СП АІ-011 до формату інтерфейсу RS-232 послідовного COM-порту ПЕОМ та зворотно. При цьому, за необхідністю, обмін інформацією можливо здійснювати також по USB-порту через перехідний пристрій з COM-порту на USB-порт. Для контролю роботи УПС у реальному масштабі часу та відповідних режимів роботи АПД СП АІ-011 розроблено СПЗ для ПЕОМ. СПЗ також дозволяє автоматично здійснювати передачу даних за необхідними режимами роботи та закривати канал зв'язку у нештатних ситуаціях.

УДК514.18:004.4

СТВОРЕННЯ СКЛАДНИХ ІНЖЕНЕРНИХ КРЕСЛЕНИКІВ З ВИКОРИСТАННЯМ ОПТИЧНОГО РОЗПІЗНАВАННЯ СИМВОЛІВ

Рябченюк Еліза, Гумен Олена, Селіна Ірина
Національний технічний університет України,
"Київський політехнічний інститут імені Ігоря Сікорського"

Анотація. Розглядається процес створення складних інженерних креслеників з використанням оптичного розпізнавання символів (OCR). Оптичне розпізнавання символів - це технологічний метод перетворення зображення тексту в редагований текстовий формат. У роботі детально розглядаються механізми функціонування OCR, включаючи отримання зображення, попередню обробку, розпізнавання тексту та подальшу обробку. Основна увага приділяється застосуванню OCR у створенні інженерних креслеників для полегшення обробки та аналізу друкованих документів.

Ключові слова. Оптичне розпізнавання символів (OCR), інженерні кресленики, механізми OCR.

Abstract. The process of creating complex engineering drawings using optical character recognition (OCR) is considered. OCR is a technological method for transforming image-based text into an editable text format. The paper delves into the mechanisms of OCR, including image acquisition, pre-processing, text recognition, and subsequent processing. The primary focus is on the application of OCR in engineering drawing creation to facilitate the processing and analysis of printed documents.

Keywords. Optical character recognition (OCR), engineering drawings, OCR mechanisms.

З розвитком технологій і зростанням присутності цифрових носіїв у сучасному світі відбулося зростання потреби в оцифрованих документах. Значні переваги перед своїми паперовими аналогами, зокрема щодо фізичного простору, який вони займають, та безпеки, пов'язаної з їх використанням, мають документи, що зберігаються у цифровому вигляді. Як результат, аналіз документів за допомогою штучного інтелекту для їх оцифрування є невід'ємною частиною комп'ютерного зору і став сферою досліджень, що швидко розвиваються.

OCR (оптичне розпізнавання символів) є ключовим елементом оцифрування документів. Визначення тексту із зображень документів дає змогу алгоритмам обробки природної мови розшифрувати текст і зрозуміти, що передає документ. Крім того, текст можна легко перекладати кількома мовами, що робить його легко інтерпретованим будь-кому. Проте OCR не обмежується виявленням тексту лише із зображень документів. Нові алгоритми OCR використовують комп'ютерний зір і NLP (обробка природної мови) для розпізнавання тексту з назв продуктів супермаркетів, дорожніх знаків і навіть з рекламних щитів, що робить їх ефективним перекладачем.

Найсучасніші нейронні мережі стали надзвичайно корисними для визначення тексту в документах і зображеннях, навіть якщо він нахилений, повернутий або перекошений.

Створення складних інженерних креслеників з використанням оптичного розпізнавання символів є важливою та інноваційною задачею, яка знаходить застосування в різних сферах, включаючи інженерію, дизайн та інші технічні області. OCR – це технологія, що дозволяє розпізнавати текст та символи на зображеннях або відео, перетворюючи їх у редагований текстовий формат.

При створенні складних інженерних креслеників застосування OCR може значно полегшити та прискорити процес роботи з технічними малюнками, схемами та планами.

Основні етапи цього процесу:

– *Сканування технічних креслень*. Початковий етап передбачає отримання цифрового зображення технічного креслення, будь то ручне малюнок або інженерний проект.

– *Використання технології OCR*. Технологія OCR використовується для автоматичного розпізнавання символів та тексту на скані. Сучасні OCR-системи можуть працювати з різними типами шрифтів та рукописним текстом.

– *Створення редагованого тексту*. Розпізнані символи перетворюються в редагований текстовий формат, який може бути подальше використаний для редагування та модифікації.

– *Інтеграція з іншими інженерними інструментами*. Одержаний редагований текст може бути інтегрований з іншими інженерними програмами та інструментами для подальшої обробки чи аналізу.

– *Перевірка та корекція*. Наостанок, важливим етапом є перевірка розпізнаних символів та можливі корекції. Це може включати в себе вручну корекцію помилок OCR або автоматизовані методи перевірки.

Розглянемо декілька особливо популярних варіантів оптичного розпізнавання інженерних креслеників:

ABBYY FineReader. Універсальне програмне забезпечення для інтерпретації креслень, яке використовує технологію OCR з можливостями розпізнавання тексту. Підтримує різні формати зображень, збереження макета, експорт даних та інтеграцію.

Adobe Acrobat Pro. Крім редагування, перегляду та керування PDF-файлами, Acrobat дозволяє сканувати документи та креслення за допомогою OCR, видобувати текст і виконувати пошук. Підтримує різні мови та дозволяє користувачам налаштовувати параметри.

Bluebeam Revu. Інша популярна програма PDF, Bluebeam Revu, використовує технології оптичного розпізнавання тексту для видобутку тексту з інженерних креслень.

AutoCAD. AutoCAD, або автоматизоване проектування, підтримує плагіни OCR для інтерпретації креслень та їхнього перетворення на редаговані елементи CAD.

PlanGrid. Програмне забезпечення, що включає оптичне розпізнавання тексту. За допомогою цієї функції можна завантажувати зображення креслення, а потім видобувати, упорядковувати, індексувати та шукати текст.

Amazon Textract. Хмарна функція AWS, яка дозволяє аналізувати документи OCR та видобувати з них елементи, такі як таблиці. Також розпізнає елементи з креслень і надає API для інтеграції з іншими програмами.

Butler OCR. API для розробників для видобутку документів, яке поєднує машинне навчання з перевіркою людини для підвищення точності розпізнавання документів.

У додаток до цих інструментів інженерії, також існує можливість розробки власних моделей машинного навчання. За допомогою фреймворків, таких як TensorFlow або PyTorch, можна налаштувати ці рішення для розпізнавання конкретних елементів плану та досягнення вищої точності, відповідно до потреб організації.

Створення складних інженерних креслеників з використанням OCR представляє собою потужний інструмент для автоматизації обробки інженерних документів. Застосування технологій OCR у поєднанні з сучасними програмами та фреймворками надає можливість швидкого та точного розпізнавання тексту, а також ефективної обробки інженерних креслень.

Програмне забезпечення, таке як ABBYY FineReader, Adobe Acrobat Pro, Bluebeam Revu, AutoCAD, PlanGrid, Text (AWS), та Butler OCR, розширює можливості інженерів та дизайнерів, забезпечуючи зручний інструментарій для редагування, аналізу та управління інженерними документами. Варто відзначити, що окрім готових рішень, індивідуальна розробка моделей машинного навчання за допомогою TensorFlow або PyTorch може відкрити нові перспективи у покращенні точності розпізнавання та адаптації до конкретних потреб організації.

Загалом, використання OCR у створенні інженерних креслеників підкреслює значущість технологічних інновацій у роботі з інженерно-технічною документацією, сприяючи ефективності та точності процесів проектування та аналізу.

Література

1. Використання OCR для складних інженерних креслень. URL: https://www.unite.ai/uk.

2. 7 Best OCR Software of 2022 (Free and PAID). URL: https://theecmconsultant.com/best-ocr-software/#nanonets.

3. ABBYY® FineReader PDF 15 User's Guide. URL: https://pdf.abbyy.com/media/1676/users_guide.pdf.

4. Порівняння програмного забезпечення для оптичного розпізнавання символів. URL: https://uk. wikipedia.org/wiki/ Порівняння_програмного_забезпечення_для_оптичного_розпізнавання_символів.

5. Optical Character Recognition Software. URL: https://www.kofax.com/products/omnipage/ocr-developer-portal.

УДК 004.492.3+ 378.147

ВИБІР ІНСТРУМЕНТАРІЮ БЛОКУВАННЯ ІНТЕРНЕТ-РЕКЛАМИ В ОСВІТНІХ ОНЛАЙН-СЕРЕДОВИЩАХ

Сербан Василь
Українська академія друкарства

У представленому дослідженні обумовлено критерії та проаналізовано розповсюджені броузерні рішення для блокування інтернет-реклами в освітніх онлайн-середовищах.

Ключові слова: мережева безпека, освітнє онлайн-середовище, інтернет-реклама, плагін.

In the presented study, the criteria and analysis of common browser solutions for blocking Internet advertising in online educational environments are determined.

Keywords: network security, online educational environment, Internet advertising, plug-in.

Цифровізація освіти визначається великою кількістю інформації, яка щодня потрапляє до поля зору студентів через інтернет. Серед цього потоку даних значне місце займає мережева реклама. Поряд з ефективним маркетингом у просуванні товарів та послуг, таргетингом цільової аудиторії та джерелом доходів для онлайн-платформ, несе негативний безпековий та етичний вплив. Перевищення кількості рекламних повідомлень може вивести студентів з концентрації та викликати розсіювання уваги. Збір та використання особистих даних для таргетингу може порушувати приватність користувачів. Деякі рекламні матеріали можуть містити неточні або обманливі відомості, що може впливати на віру студентів у мережеву інформацію. Агресивна або неприємна реклама може негативно впливати на ментальне здоров'я користувачів, особливо в уразливих групах. Для ефективного вирішення обумовлених проблем важливо розглядати мережеву рекламу в контексті не лише маркетингу, але й психології та соціології. Тільки за таких умов можна досягти балансу між ефективністю рекламної кампанії та збереженням уваги та концентрації студентів. Етичні наслідки поглиблюються через відсутність ефективного контролю та регулювання в сфері мережевої реклами в освітньому онлайн-середовищі. Отже, визначення механізмів для моніторингу та забезпечення дотримання етичних стандартів та вибір інструментарію блокування інтернет-реклами в освітніх онлайн-середовищах є своєчасним та актуальним.

Враховуючи негативні наслідки цього явища, у вищій школі виникає необхідність у розробці та впровадженні ефективних засобів для повного усунення впливу мережевої реклами на освітній процес. Передусім важли-

во розробити та впровадити суворі правила та політики, які обмежать використання мережевої реклами в освітньому онлайн-середовищі. Ці положення повинні визначати межі та обмеження для рекламних матеріалів, зокрема враховувати їх вплив на контент та користувачів.

Освітнє онлайн-середовище потребує ефективних інструментів для блокування реклами та нормалізації робочого процесу. Зовнішні розширення та плагіни для різних браузерів виконують цю функцію найкраще з розглянутих засобів, забезпечуючи користувачам можливість фокусуватися на навчанні без відволікань. У представленому дослідженні обумовлено критерії та проаналізовано розповсюджені броузерні рішення для блокування інтернет-реклами в освітніх онлайн-середовищах (таблиця).

Розширення *AdBlock Plus* надає можливість блокування рекламних елементів на веб-сайтах [1]. Засноване на фільтрах EasyList, воно дозволяє користувачам ефективно контролювати відображення реклами. Також має можливість створювати правила для блокування реклами на конкретних освітніх веб-сайтах, забезпечуючи ретельне уважне навчання. *uBlock Origin* є легким та швидким розширенням, спрямованим на ефективне блокування рекламних елементів [2]. Відмінно впорається із завданням оптимізації ресурсів та швидкістю браузера. Його функціонал дозволяє активно фільтрувати та керувати використанням ресурсів, що особливо корисно в освітньому контексті. *AdGuard* не лише блокує рекламу, але й надає додатковий захист від відстеження та шкідливого вмісту, що важливо для безпеки в освітньому середовищі, дозволяючи користувачам встановлювати настроювані правила для блокування реклами на конкретних освітніх серверах [3]. *CyberGhost* може виявитися відмінним вибором, оскільки він комбінує функціональність VPN із захистом від реклами та трекінгу на високому рівні [4]. Це додаткова функція, яка може бути корисною для освітніх платформ, що потребують інтегрованого захисту від нав'язливої реклами та слідкування в Інтернеті. *PIA MACE* призначений для блокування реклами та небезпечних доменів на рівні системи [5]. *NordVPN* фокусується на захисті конфіденційності та безпеці в Інтернеті шляхом шифрування з'єднань та приховання IP-адрес користувачів. Вбудованою технологією блокування реклами та відстеження, а також фокусом на конфіденційності та швидкості перегляду в Інтернеті визначається ресурс *Brave Browser*: функція "Brave Shields" надає користувачам додатковий контроль над тим, яка реклама та відстеження блокуються на конкретних вебсайтах [6]. Програмне забезпечення *Pi-hole* використовується для блокування мережевої реклами, фільтруючи запитання DNS та блокуючи доступ до доменів, пов'язаних із нав’язливою рекламою та трекінгом [7]. Це відбувається до того, як вебсторінка з освітнім контентом завантажиться, що дозволяє ефективно блокувати рекламу перед тим, як вона відкриється студентам.

Критерії аналізу / Плагіни блокування	Логотип бренду	Блокування броузерної реклами	Блокування трекера	Шифрування даних	Приховування IP	Блокування реклами YouTube	Відсутність реєстрації
CyberGhost		В	В	+	+	+	+
PIA MACE		В	В	+	+	+	+
NordVPN		В	В	+	+	+/—	+
AdGuard		В	В	—	—	+	—
Brave Browser		В	С	—	—	+	—
uBlock Origin		В	С	—	—	+	—
Pi-hole		В	С	—	—	—	—
Adblock Plus		В	С	—	—	+	—
AdBlock		С	Н	—	—	+	—

Проаналізовані розширення та плагіни для блокування реклами і нормалізації роботи в освітньому онлайн-середовищі надають різноманітні інструменти для оптимізації університетських платформ, усуваючи негативний вплив інтернет-реклами. Вони дозволяють ефективно керувати вмістом, захищати приватність та забезпечувати невідволіканне навчання в онлайн-середовищі. Таким чином, створення та підтримка освітніх середовищ з очищеним вмістом, які гарантують відсутність рекламних елементів, може бути ключовим кроком у повному усуненні впливу мережевої реклами в онлайн-освіті. Такі платформи забезпечують навчання та взаємодію без додаткових відволікань. Застосування суворих правил, технологічних рішень, розвиток очищених освітніх рішень та участь у глобальних ініціативах стануть основою для створення етичного та продуктивного академічного простору.

Література

1. Adblock Plus | The world #1 free ad blocker. URL: adblockplus.org
2. uBlock Origin - Free, open-source ad content blocker. URL: ublockorigin.com
3. AdGuard — найсучасніший блокувальник реклами у світі! URL: adguard.com
4. Fast, Secure & Anonymous VPN service | CyberGhost VPN. URL: cyberghostvpn.com
5. Private Internet Access: The #1 Best VPN Service For 10+ Years. URL: privateinternetaccess.com
6. Secure, Fast, & Private Web Browser with Adblocker | Brave. URL: brave.com
7. Pi-hole & Network-wide Ad Blocking. URL: pi-hole.net

УДК 001+0.034+004.5

ПІДВИЩЕННЯ ЯКОСТІ ПРОВЕДЕННЯ ЗАНЯТЬ У ЗАКЛАДАХ ОСВІТИ ШЛЯХОМ ЗАСТОСУВАННЯ SMART-ТЕХНОЛОГІЙ

Синчук Іван, Романик Андрій, Гук Олег
Вище професійне училище Львівського державного університету безпеки життєдіяльності (м. Вінниця)

Анотація. *У тезах доповіді аналізується використання SMART-технології в освітньому процесі.*

Під час написання було відзначено затребуваність високого рівня цифрової грамотності та ІТ-компетентності з боку, як викладачів так і здобувачів освіти, можливість закладів освіти забезпечувати достатній рівень навчання здобувачів не тільки на загальноосвітньому, а і на вузькопрофесійному рівні. Що стосується здобувачів, то для ефективності «розумного навчання», окрім вказаного, необхідно мати достатній рівень самоконтролю, самоорганізації та вміння користуватися інформацією.

Ключові слова: *SMART-технології, інформаційно-комунікативні технології, сучасні технології викладання, електрона освіта (e-learning), розумне навчання (Smart Education).*

Соціальна інформатизація це глобальний соціальний процес, що характеризується збором, накопиченням, удосконаленням, обробкою, зберіганням, використанням, прийомом та передачею інформації, є провідною діяльністю у сфері суспільного виробництва. Вище наведенні процеси здійснюються на базі новітніх та сучасних інформаційно-комунікативних технологій, а також на основі різноманітних засобів обробки та обміну інформацією.

Розвиток та реформування сучасної освіти не стоїть на місці, так в XX столітті акцент був сформований на інформаційні технології, а от у XXI столітті на інформаційно-комунікативні технології. В даний час відбувається перехід від e-learning до Smart (англ. - розумний, кмітливий, енергійний) e-learning і Smart Education (розумне навчання).

Розумне навчання (англ. *Smart Education*) – це гнучке навчання в інтерактивному освітньому середовищі за допомогою контента з усього світу, що знаходиться у вільному доступі. Отже, інформація стає доступна, як для викладача так і для здобувача освіти.[1].

SMART-технології це інтерактивний комплекс, який дає змогу здобувачеві освіти дистанційно та самостійно опрацювати навчальний матеріал, мотивує їх до пізнавальної діяльності та забезпечує вільний доступ для використання освітніх ресурсів, як для викладачів так і для здобувачів освіти під час аудиторних та поза аудиторних занять.

Всебічне застосування та впровадження SMART – технологій в освітній процес дає змогу:

- швидко знаходити, аналізувати та використовувати необхідну інформацію;
- збільшувати обсяг навчальної інформації у всесвітній мережі «Internet»;
- ділитися інформацією між викладачами та здобувачами освіти;
- висвітлювати яскраві презентації, демонструвати інформацію з всесвітньої мережі «Internet» або відео на інтерактивному екрані;
- підвищити рівень використання інноваційних технологій, як у навчанні так і в повсякденному житі;
- проводити інтерактивне тестування (опитування) здобувачів освіти;
- активізувати здобувачів освіти до пізнавальної діяльності та самостійного навчання.

Для здійснення розумного навчання в освітньому процесі необхідне використання сучасних інтерактивних технологій та технологій здійснення освітнього процесу з застосуванням креативної освіти таких, як: SMART Board, SMARTart, SMART Classroom, **SMART Exchange**, віртуальні лабораторії з використанням SMART – технологій.

Найбільше в закладах освіти використовують інтерактивні дошки тому що вони дозволяють реалізувати один з найважливіших принципів навчання – наочність. Також хочеться зазначити що заняття з використанням інтерактивних дощок стає більш цікавим, веселим та захоплюючим. Звичайно, для максимальної реалізації всіх властивостей інтерактивних дошок створено різноманітне спеціальне програмне забезпечення таке, як: SMART Notebook, Bridgit, Synhron Eyes.[2]. У кожного вище зазначеного програмного забезпечення є свої особливості, а також плюси та мінуси.

В нашому закладі освіти найбільшу популярність має програмне забезпечення – SMART Notebook, отже розглянемо цікаву особливість даної програми для проведення, як аудиторної так і поза аудиторної роботи, а саме процеси для створення завдань:

– *Заповнення пропусків* – здобувачі освіти перетягують слова або числа в порожні поля, що дає можливість розвивати дедукцію, навичку компонування та послідовність мислення. Дане завдання може слугувати, як для підведення підсумків по заняттю так і для опитування по раніше вивченому матеріалу.

Алгоритм створення процесу «Заповнення пропусків»

– *Ігрове шоу* – дає можливість створити тестове опитування у формі гри, здобувачі освіти відповідають на поставленні питання з скількома запропонованим відповідями. Запитання будуються у такі формі щоб на них можливо було відповісти у формі «правда чи брехня» або вибрати правильний варіант із декількох запропонованих відповідей. Дане завдання може слугувати для проведення вікторин, конкурсів, олімпіад, а також це цікавий спосіб пригадати навчальний матеріал у формі гри.

Алгоритм створення процесу «Ігрове шоу»

– *Поєднайте їх!* – здобувачі освіти підбирають пов'язані між собою елементи. Дане завдання дає можливість розвивати у здобувачів освіти навички взаємно-однозначної відповідності та тренувати короткочасність пам'яті, а також для перевірки знань у здобувачів освіти по вивченому матеріалу.

Алгоритм створення процесу «Поєнайте їх»

SMART освіта має всі передумови для того, щоб стати найбільш ефективною інноваційною моделлю здійснення освітньої діяльності в умовах глобального інформаційного суспільства. Головною ознакою цієї освітньої моделі є система гнучкого навчання в інтерактивному освітньому середовищі, що дозволяє здійснити перенесення частини освітнього процесу в електронне середовище.[1].

У підсумку можна констатувати той факт, що з використанням SMART-технологій навчання набуває нової якості, навчання є вмотивованим, а викладання є інтерактивним, тобто включає фото-, відео фрагменти, зовнішні електроні ресурси, анімацію тощо, доступ до яких здобувачі освіти можуть отримати за допомогою своїх гаджетів. Отже застосування SMART-технологій потребує чіткої структури навчання та відповідного програмного забезпечення, а також важливого значення набуває знання викладача сучасних інтерактивних технологій та технологій здійснення освітнього процесу із застосуванням креативної освіти.

Література:

1. Електроний ресурс: http://smarteducatoin.blogspot.com/2016/06/smart-education.html).

2. Електроний ресурс: Smart технології в освіті – Смарт технології (google.com).

УДК 004.42

ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА ОБЛІКУ ПРОТИПОЖЕЖНОГО СТАНУ ОБ'ЄКТА

Сировий В., Придатко О.
Львівський державний університет безпеки життєдіяльності

Наведено огляд інформаційно-аналітичної системи «Інтерактивний інспектор» у вигляді чат-боту для автоматизації процесів оцінки протипожежного стану об'єктів. Обґрунтовано її необхідність та затребуваність на українському ринку.

Ключові слова: чат-бот, Java, Spring, Hibernate, Telegram API, перевірка, алгоритм, пожежна безпека, закон №3361, страхове покриття, ДСНС.

An overview of the "Interactive Inspector" information and analytical system in the form of a chatbot for automating the processes of assessing the fire safety condition of objects is given. Its necessity and demand on the Ukrainian market are substantiated.

Key words: chat-bot, Java, Spring, Hibernate, Telegram API, audit, alrogithm, fire safety, low №3361, insurance coverage, SES.

6 жовтня 2022 року Президент України підписав закон №3361 [1], який вніс зміни в сферу пожежної безпеки. Цей закон відмінив перевірки Державної служби з надзвичайних ситуацій (ДСНС) для бізнесів із середнім та/або незначним ступенем ризику, що мають страховий захист від пожеж. Згідно з законопроєктом, якщо бізнес отримав страховий поліс відповідальності, то він звільняється, на період дії цього полісу, від перевірок. [2] Тобто суб'єктам господарювання потрібно буде провести аудит пожежної безпеки та оформити страхування. Потім повідомити ДСНС про наявність страхування та на період дії договору звільнитися від планових пожежних перевірок. Ця ініціатива надає підприємцям можливість самостійно обирати необхідне обладнання відповідно до вимог щодо пожежної безпеки. Це величезний прорив, щоб мінімізувати корупцію.

Проте, більшості підприємців здебільшого не зрозумілі норми та правила відповідно до яких проводиться перевірка відповідності правилам пожежної безпеки. У зв'язку з цим виникла необхідність у системі, яка зможе покрити потреби користувачів у визначенні вимог щодо пожежної безпеки у декілька кроків. Інтерактивний інспектор – швидкий та зручний чат-бот, який базується на власноруч розроблених алгоритмах для багатопараметричної оцінки протипожежного стану об'єкта, заснованих на аналізі понад тридцяти нормативних документів. Продукт спрямований на страхові компанії, підприємців та суб'єктів господарювання, які можуть провести незалежну оцінку протипожежного стану. Також, цей проект призначений для посадових осіб ДСНС, які здійснюють державний нагляд (контроль) у сфері техногенної та пожежної безпеки.

Проект реалізовано за допомогою об’єктно-орієнтованої мови програмування Java. Задля зручності у написанні коду, роботі з Telegram API та розгортанні програми використано фреймворк Spring. У якості СУБД є об’єктно-реляційна система керування PostgreSQL. Для ефективного керування реляційними даними Java код взаємодіє з базою даних за допомогою фреймворку Hibernate, який надає простий у використанні API.

Інтерактивний інспектор автоматизує такі основні процеси:

- вибір типу та необхідної кількості вогнегасників для об’єкта;
- визначення необхідності проектування та монтажу автоматичних систем пожежної сигналізації та пожежогасіння;
- визначення типу системи оповіщення, її характеристик та управління евакуацією при пожежі;
- врахування необхідності систем протидимного захисту;
- визначення ступеня ризику від провадження господарської діяльності;
- визначення категорій приміщень, будинків, установок за вибухопожежною та пожежною небезпекою;
- визначення класів пожеж;
- визначення класу зони;
- визначення необхідності влаштування та параметрів внутрішнього й зовнішнього протипожежного водопостачання;
- визначення протипожежних відстаней між будівлями, технологічними установками, інженерними комунікаціями;
- визначення допустимої поверховості та площі протипожежного відсіку;

Висновок: вступ в дію закону №3361 від 6 жовтня 2022 року став кроком у напрямку покращення пожежної безпеки в Україні, надавши підприємцям можливість самостійно обирати протипожежне обладнання відповідно до вимог безпеки. У цьому контексті виникла необхідність у системі, що допомагає визначати вимоги до пожежної безпеки. Розроблений чат-бот «Інтерактивний інспектор» на базі Java з використанням Telegram API та фреймворку Spring надає зручний та швидкий спосіб оцінки протипожежного стану об'єктів, спрямований на страхові компанії та суб'єкти господарювання. Цей проект автоматизує ключові процеси визначення вимог щодо пожежної безпеки, сприяючи ефективному управлінню ризиками та виконанню вимог законодавства.

Література

1. Проект Закону про внесення змін до деяких законодавчих актів України щодо перших кроків дерегуляції бізнесу шляхом страхування цивільної відповідальності : Закон України №3361-IX від 17.04.2020 р. – Режим доступу до ресурсу: https://itd.rada.gov.ua/billInfo/Bills/Card/1995

2. Український бізнес звільняють від перевірок із ДСНС : веб-сайт – Режим доступу до ресурсу: https://business.diia.gov.ua/cases/novini/ukrainskij-biznes-zvilnat-vid-perevirok-iz-dsns (дата звернення 20.11.2023)

УДК 681.5+004.75

СУЧАСНІ ПІДХОДИ ДО УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ СИСТЕМАМИ

Смик Денис, Бурак Назарій
Львівський державний університет безпеки життєдіяльності

Динаміка росту процесів інтеграції інформаційних технологій в усі сфери діяльності суспільства зумовлює стрімкий ріст генерації великих обсягів інформації, яка потребує оперативної обробки з метою подальшого збереження та використання. У зв'язку з цим актуалізується питання пошуку нових методів та засобів ефективного управління інформаційними системами. Високу ефективність при вирішення задачі оперативності обробки та зберігання даних демонструють системи основані на технології розподілених та паралельних обчисленнях.

Ключові слова: розподілене зберігання, паралельні обчислення, децентралізовані алгоритми, інформаційні технології, дані.

The growth dynamics of information technology integration processes in all spheres of society's activities leads to a rapid growth in the generation of large volumes of information that requires operational processing for the purpose of further storage and use. In this regard, the issue of finding new methods and means of effective information systems management is becoming more relevant. Systems based on the technology of distributed and parallel computing demonstrate high efficiency in solving the problem of operational data processing.

Key theses: distributed storage, parallel computing, decentralized algorithms, ensuring security and privacy and development prospects and future challenges.

Під інформаційною системою у сучасному трактування нормативно правових актів розуміють "комунікаційну система, що забезпечує збирання, пошук, оброблення та пересилання інформації". Така система передбачає сукупність організаційних і технічних засобів для обробки та збереження інформації з метою забезпечення інформаційних потреб користувачів, якими можуть виступати як люди, так і машини або інші інформаційні системи.

Загальна класифікація таких систем здійснюється за такими ознаками: за ступенем автоматизації, за сферою призначення, за місцем діяльності та за функціональним призначенням(див. Рис. 1).

Залежно від рівня автоматизації виділяють ручні (усі операції обробки інформації здійснюються оператором-людиною), автоматизовані(функції обробки здійснюються за певним алгоритмом, який передбачає часткову автоматизацію процесів) й автоматичні інформаційні системи (усі функції керування й опрацювання даних здійснюються технічними засобами без участі людини (наприклад, автоматичне керування технологічними процесами))

Рисунок 1 – Критерії класифікації інформаційних систем

Сучасні темпи розвитку суспільства, кількість даних спровокована наступною хвилею "інформаційного вибух" диктують свої умови для зміни технології їх обробки та зберігання. Динаміка росту інформаційних ресурсів зумовлює появу нових проблем, пов'язаних із їх використанням та управління інформаційними системами. Одним із шляхів вирішення зазначених перешкод є застосування розподіленого принципу обробки та зберігання даних.

Автоматизоване управління інформаційними системами (далі - АУІС) на основі розподілених технологій є перспективним напрямком в розвитку ефективних та стійких інформаційних платформ. Цей підхід переосмислює традиційні методи управління даними та впроваджує інновації, забезпечуючи більшу продуктивність та адаптивність інформаційних систем до умов сьогодення.

Однією з фундаментальних особливостей інтеграції розподілених технологій в АУІС є розподілене зберігання даних. Такий підхід передбачає розміщення інформації на різних вузлах мережі, що забезпечує високу швидкість доступу та стійкість до відмов. Це особливо важливо в умовах обробки великих обсягів даних, коли запити на доступ до інформації реалізуються із використання принципу паралельності.

Паралельні обчислення використовуються для розділення завдань на менші частини, що обробляються в один момент часу. Застосування технологій розподілених технологій управління інформаційними системами стають необхідним елементом для забезпечення їх ефективності в режимі реального часу. Це дозволяє значно прискорити час виконання завдань та підвищити продуктивність інформаційної системи, а їх гнучкість та стійкість забезпечується інтеграцією децентралізованих алгоритмів в програмне забезпечення управління.

Таким чином, застосування сучасних методів та інструментарію оброблення даних у контексті автоматизованого управління інформаційними

системами, що базуються на розподілених технологіях, є критичним для ефективності та надійності функціонування таких систем. Використання цих підходів дозволяє підвищити швидкість прийняття рішень, забезпечити високу доступність та оптимальне використання ресурсів.

Розподілені технології не лише визначають новий етап розвитку управління інформаційними системами, але й стають необхідним кроком для адаптації до вимог сучасного інформаційного суспільства. Автоматизоване управління на їхній основі відкриває нові перспективи для оптимізації бізнес-процесів та забезпечення стабільності інформаційних систем у невизначеному та швидкозмінному світі.

Література

1. Parallel computing in the computing cluster [Електронний ресурс]. – Доступний з https://medium.com/@abdulkaderhajjouz/parallel-computing-in-the-computing-cluster-in-depth-b9f9f8ee283

2. Blockchain based decentralized [Електронний ресурс]. – Доступний з https://www.sciencedirect.com/science/article/pii/S2352484721007204

3. Eremina, Luba & Mamoiko, Anton & Aohua, Guo. (2023). Application of distributed and decentralized technologies in the management of intelligent transport systems. Intelligence & Robotics. 3. 149-61. DOI:10.20517/ir.2023.09.

4. Samoylenko, H.T. & Selivanova, A.V.. (2023). Distributed information systems in e-commerce. Mathematical machines and systems. 2. 69-74. DOI:10.34121/1028-9763-2023-2-69-74. Науковий вісник НЛТУ України, 30(5), 105-113. https://doi.org/10.36930/40300518

5. Придатко О. В., Бурак Н. Є., Дзень В. Є., Кунинець М. С. Адаптивна інформаційно-довідкова система "UniBell" як складова частина проєкту "Smart-університет". Науковий вісник НЛТУ України. 2020, т. 30, № 5. С. 105–113

УДК 351.861

ОБГРУНТУВАННЯ ПРОПОЗИЦІЙ ЗА РЕЗУЛЬТАТАМИ АНАЛІЗУ БАГАТОФАКТОРНИХ МОДЕЛЕЙ ГУМАНІТАРНОГО ПІДВОДНОГО РОЗМІНУВАННЯ

***Соловйов Ігор*, Соловйов Павло, Стрілець Віктор**
ГУ ДСНС України в Херсонській області, НУЦЗУ

Анотація. Показано, що наявність багатофакторних моделей гуманітарного підводного розмінування (підйому вибухонебезпечного предмету, підводного підриву вибухонебезпечного предмету, підйому вибухонебезпечного предмету за допомогою спеціалізованого пристрою) дозволило обґрунтувати оперативно-технічні рекомендації щодо підвищення ефективності діяльності водолазів-саперів ДСНС з визначеним рівнем значимості.

Ключові слова. Гуманітарне підводне розмінування, багатофакторна математична модель, аналіз.

Abstract. It is shown that the presence of multifactorial models of humanitarian underwater demining (lifting an explosive object, underwater detonation of an explosive object, lifting an explosive object using a specialized device) made it possible to substantiate operational and technical recommendations for increasing the efficiency of the activities of divers-sappers of the State Emergency Service with a certain level of significance.

Keywords. Humanitarian underwater demining, multifactorial mathematical model, analysis.

Незважаючи на те, що існуючий рівень технологічного прогресу дозволяє на протязі між 2010 та 2030 роками на 100% збільшити використання водних ресурсів, всі прибережні країни ЄС зіткнулись з викликами, що пов'язані із повоєнними залишками вибухонебезпечних та хімічних речовин у водних акваторіях. Крім цього у всьому світі на цей час встановлено біля 70 мільйонів мін, з яких, ймовірно, 15% встановлені на мілководні ділянки внутрішніх водоймищ. В Україні ці виклики усугубляються як значною кількістю вибухонебезпечних предметів на узбережжі Чорного та Азовського морів, характерним прикладом чого є Херсонська область, особливо після підриву рашистами Каховської ГЕС, так і збільшенням вибухонебезпечних предметів (ВНП), які забруднюють мирні водні акваторії внаслідок агресії Росії.

Визначено, що важливою та нерозв'язаною частиною цієї проблеми є відсутність науково-методичного апарату обґрунтування пропозицій щодо підготовки особового складу ДСНС до підводного розмінування за результатами аналізу багатофакторних імітаційних моделей, у тому разі, коли це стосується питання попередньої оцінки того, наскільки ефективним буде проведення оперативної роботи за допомогою нових технічних засобів.

В доповіді розглядаються отримані авторами трифакторні квадратичні моделі в нормованих перемінних гуманітарного підводного розмінування (ГПР), для яких була підтверджена достовірність з рівнем значимості α=0,05:

– підйому вибухонебезпечного предмету

$$y_{\text{підйом}} = 0{,}449 - 0{,}158 \cdot x_1 - 0{,}285 \cdot x_2 - 0{,}057 \cdot x_3 + 0{,}054 \cdot x_1^2 + \\ + 0{,}077 \cdot x_2^2 - 0{,}059 \cdot x_1 \cdot x_2 - 0{,}021 \cdot x_1 \cdot x_3 + 0{,}004 \cdot x_2 \cdot x_3 , \quad (1)$$

– підводного підриву вибухонебезпечного предмету

$$y_{\text{підрив}} = 0{,}412 - 0{,}153 \cdot x_1 - 0{,}307 \cdot x_2 - 0{,}043 \cdot x_3 + 0{,}046 \cdot x_1^2 + \\ + 0{,}065 \cdot x_2^2 - 0{,}033 \cdot x_1 \cdot x_2 - 0{,}001 \cdot x_1 \cdot x_3 - 0{,}0005 \cdot x_2 \cdot x_3 \quad (2)$$

– підйому вибухонебезпечного предмету із застосуванням спеціалізованого пристрою

$$y_{\text{кошик}} = 0{,}440 - 0{,}227 \cdot x_1 - 0{,}201 \cdot x_2 - 0{,}065 \cdot x_3 + \\ + 0{,}068 \cdot x_1^2 + 0{,}061 \cdot x_2^2 - 0{,}059 \cdot x_1 \cdot x_2 - 0{,}044 \cdot x_1 \cdot x_3 + 0{,}020 \cdot x_2 \cdot x_3 \quad (3)$$

де x_1 – рівень підготовленості водолаза-сапера; x_2 – рівень оснащеності; x_3 – умови, в яких працює особовий склад.

Аналіз (1) показав, що при рівні значимості двостороннього ризику α=0,01 можна говорити, що на час підйому ВНП особовим складом ДСНС тільки рівень підготовленості x_1 та умови проведення підводного розмінування x_2. В той же час з рівнем значимості α=0,05 можна стверджувати, що під час розробки оперативно-технічних рекомендацій водолазам-саперам необхідно додатково враховувати як тип водолазного костюму x_3, так і ефекти взаємодії між рівнем підготовленості особового складу та умовами, в яких вони працюють. В той же час можна не враховувати ефекти взаємодії умов підйому ВНП з тим, в якому костюмі працюють водолази сапери, а також квадратичний ефект від застосування сухого чи мокрого костюму. Слід очікувати, що у випадку підйому ВНП підвищення рівня підготовленості більш сильно буде проявлятись у водолазів-саперів з первинним рівнем, як і те, що саме для них на зниження ефективності підводного розмінування будуть впливати погані зовнішні умови роботи.

Аналіз (2), що вже при рівні значимості двостороннього ризику α=0,01 можна говорити, що на час підводного підриву ВНП особовим складом ДСНС впливають тільки рівень підготовленості x_1 та умови проведення підводного розмінування x_2. Ця ж ситуація остається і за рівня α=0,05 та α=0,1. В той же час, враховуючи те, що під час проведення пошукових досліджень, а дослідження систем «водолаз-сапер – технічне забезпечення гуманітарного розмінування – умови підводного підриву вибу-

хонебезпечного предмету» відносяться саме до таких, можна давати висновки з рівнем значимості до 0,2, доцільно звернути увагу на те, що в практичній діяльності необхідно враховувати ефекти взаємодії між умовами здійснення підводного підриву ВНП та рівнем підготовленості водолазів-саперів, квадратичні (нелінійні) ефекти для цих значимих факторів (тобто підвищену увагу потрібно звернути на підготовку водолазів-саперів до роботи в складних умовах та на планування оперативної діяльності спеціалізованого піротехнічного підрозділу), а також те, що поява нових технічних засобів забезпечення ГПР може суттєво вплинуть на ефективність його проведення. Тобто, під час розробки оперативно-технічних рекомендацій водолазам-саперам ДСНС щодо підвищення ефективності здійснення підводного підриву вибухонебезпечних предметів в першу чергу необхідно звернути увагу на покращення рівня підготовленості особового складу та умови проведення гуманітарного підводного розмінування. Поряд з цим також необхідно враховувати спорядження водолазів-саперів, а також ефекти взаємодії між рівнем підготовленості особового складу та умовами, в яких вони працюють. Слід очікувати, що у випадку підводного підриву вибухонебезпечного предмету підвищення рівня підготовленості більш сильно буде проявлятись у водолазів-саперів з первинним рівнем, як і те, що саме для них на зниження ефективності підводного розмінування будуть сильніше впливати погані зовнішні умови роботи.

Аналіз виразу (3) та його порівняння з (1) показало, що у випадку використання спеціалізованого пристрою суттєво зменшується вплив фактору x_2, який характеризує зовнішні умови подолання надзвичайної ситуації. А саме така задача ставилась за результатами аналізу багатофакторної моделі загальноприйнятого процесу підводного розмінування. Одночасно більш важливим став фактор x_1 підготовленості водолазів-саперів у порівнянні, що свідчить про необхідність спеціальних занять по застосуванню спеціалізованого пристрою в процесі проведення гуманітарного підводного розмінування. В той же час з рівнем значимості α=0,05 можна стверджувати, що в обох випадках під час розробки оперативно-технічних рекомендацій водолазам-саперам необхідно додатково враховувати як тип водолазного костюму x_3, так і ефекти взаємодії між рівнем підготовленості особового складу та умовами, в яких вони працюють.

УДК 004.032.26

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ПОВЕДІНКУ ТА ПСИХОЛОГІЮ ЛЮДИНИ

Соромля Я. І. Дейнеко А.О.
Приватний заклад вищої освіти ІТ СТЕП Університет, Україна, Львів

Анотація. Технології штучного інтелекту зараз стрімко розвиваються, знаходять застосування у всіх аспектах життя, міняють суспільство. Але разом з тим вони міняють самих людей. У цій доповіді розглядаються питання впливу взаємодії зі ШІ на людину, здатність комп'ютерних систем направлено змінювати поведінку людини, а також використання цих технологій у психології.
Ключові слова: інформаційні технології, штучний інтелект, ШІ, технології та ментальне здоров'я, ІТ, цифровий вплив, ризики ШІ.

Abstract. Artificial intelligence technologies are currently developing rapidly, finding applications in all aspects of life, and changing society. But at the same time, they change the people themselves. This presentation examines the impact of interaction with AI on a person, the ability of computer systems to change human behavior, as well as the use of these technologies in psychology.
Keywords: AI, artificial intelligence, machine learning, psychology, mental health

Вступ. Поняття штучного інтелекту та нейронних мереж існувало досить давно. Але тільки в останні роки воно вийшло з вузького кола дослідницьких відділів корпорацій та університетів у широкий загал. Користувачам насамперед відомі такі мовні моделі як ChatGPT та Bard, генеративні моделі для зображень — найпопулярніші з них — DALL-E та MidJourney. Незважаючи на нещодавну появу, вони вже мають значний вплив на суспільство, який в майбутньому буде тільки зростати. Будуть переформатовані цілі галузі, можливо, деякі професії, популярні сьогодні, відійдуть у минуле, натомість з'являться нові можливості. Потенціал цієї технології величезний і зараз все, що пов'язане з штучним інтелектом швидко розвивається в технологічному плані. Але не слід забувати, що поки що, користувачем даних технологій є людина. Тому в цій доповіді ми розглянемо таку актуальну тему як вплив штучного інтелекту на поведінку людини, а також психологічні особливості взаємодії з нейронними мережами. Автори переконані, що актуальність даної теми буде тільки зростати і по ній в самому найближчому майбутньому буде проведено немало досліджень та написано немало наукових праць.

Метою дослідження цієї доповіді є розгляд та виокремлення тенденцій впливу штучного інтелекту на психологію людини, поведінкові та етичні аспекти взаємодії з ШІ, а також його застосування у психології, допомозі в підтриманні психічного здоров'я, профілактиці небажаних станів.

1. Негативний вплив штучного інтелекту на людину

З ростом кількості користувачів популярних нейронних мереж ми вже

можемо предметно говорити який вплив дана технологія має на ментальне здоров'я людини. Слід зазначити, що крім безумовно позитивного ефекту, що полягає у збільшенні продуктивності та доступі до узагальненої інформації без прив'язки до мови, користувачі також можуть відчувати негативні емоції, наприклад занепокоєння — через те, що вони не розуміють, як працює технологія та чого очікувати від неї. Інколи спостерігається страх - втратити роботу, бути витісненим з професії, або страх банальної невідомості та ймовірних змін. В той же час надмірне використання систем ШІ може призвести до залежності. Люди можуть відчувати потребу постійно перевіряти свої пристрої для використання програм на базі ШІ, що негативно впливає на інші сфери життя. У цьому плані залежність від смартфонів як явище була і раніше, нові можливості лише доповнюють її. Інколи спілкування з нейронними мережами викликає депресію через відчуття безпорадності та меншовартості, так як ШІ сприймається як кращий та здібніший за людину. Революційність технології та її швидке впровадження у деякої категорії користувачів викликає параною, недовіру до автоматизованих систем, особливо, коли вони керують фізичними об'єктами, такими як автономні транспортні засоби чи системи зброї. Повстання машин або не менш катастрофічні сценарії, коли роботи забирають у людини право прийняття рішень — часто фігурують у науковій фантастиці і вже стали частиною поп-культури. Упереджене негативне ставленню до ШІ не виникає на пустому місці — а підкріплюється фактами — наприклад відео-підробки, діпфейки, маніпуляції з голосом. Алгоритми соціальних мереж чи пошукових систем, розвинені настільки, що створюють цифровий портрет людини для показу релевантної реклами, за відгуками досить ефективні та насторожують. Ігри та віртуальна реальність на основі ШІ створюють відчуття занурення та втечі від реальності, що призводить до залежності та відсторонення від досвіду реального життя.

2. Вплив штучного інтелекту на поведінку людини

Для компаній, ШІ забезпечує перехід від простих алгоритмів до складних систем, заснованих на великих обсягах даних. У сфері реклами це виливається у вивченні поведінки людей для персоналізації реклами. Але, логіка показує, що наступним після вивчення поведінки є намагання змінити її. Тобто нейронну мережу можна натренувати та визначати вразливі звички або патерни поведінки людини, щоб вплинути на її прийняття рішень.

Дослідження були проведені у австралійській науковій агенції CSIRO Data61 (Commonwealth Scientific and Industrial Research Organisation's Data61), у одному з експериментів учасники повинні були вибрати червоні або сині коробки щоб вибрати фальшиву валюту. Нейронна мережа (рекурентного типу з підкріпленням) у свою чергу, зі збільшенням кількості спроб вивчає шаблон вибору учасника та скеровує його до вибору конкретного варіанту, успіх ШІ тут досягав 70%. Прикладного характеру експеримент проводила сінгапурська компанія Fujitsu, що використовує власну систему ШІ Zinrai. За допомогою програми

для смартфонів зі штучним інтелектом вони намагались вплинути на поведінку користувачів, неявно переконуючи відкласти подорож у торгові центри, стадіони і великі заходи у час пік, щоб зменшити затори.

Дані експерименти показують можливість впливу на поведінку людини, а це з одного боку дає нові інструменти для проведення державної та соціальної політики, дозволяє розпізнавати неправильний вибір людей і працювати над його корекцією, але з іншого боку ставить питання про свободу волі та свободу вибору.

3. Використання ШІ для покращення психічного здоров'я

Одним із медичних застосувань ШІ є галузь охорони психічного здоров'я. Основною складністю тут є відсутність точної та чіткої моделі практично для будь-якого психіатричного розладу. Тут застосування машинного навчання до великих даних може допомогти. Першим кроком на цьому шляху є діагностика. Психічні захворювання краще лікувати або навіть запобігти, якщо вони виявлені на ранній стадії. ШІ тут може допомогти виявити які люди знаходяться у групі ризику, а також виявити демографічні тенденції та змінні, на які можуть бути спрямовані соціальні програми для зниження захворюваності на психічні розлади. Для лікування психічних захворювань системи машинного навчання також мають ряд переваг. Тут насамперед стає можливою розробка персоналізованих програм лікування, які враховують індивідуальні потреби кожного пацієнта, його історію хвороби, симптоми, генетичні фактори, що підвищує ефективність лікування та зменшує побічні ефекти. Розробляються віртуальні терапії, що дозволяють пацієнтам отримувати терапію дистанційно. Наприклад пацієнту через технології віртуальної реальності допомагають ефективно справлятись з модельованими тривожними ситуаціями, або через використання спеціальних програм можливе навчання пацієнтів новим способам мислення та поведінки — це називається терапія комп'ютерної поведінки. Проте, віртуальні терапії все ще перебувають на ранній стадії розвитку. ШІ також можна використовувати при розробці нових методів фармакологічного лікування: для ідентифікації нових мішеней при лікуванні психічних захворювань, для врахування індивідуальних потреб кожного пацієнта.

4. Недоліки штучного інтелекту в психології

У сфері психології вивчення людських емоцій та переживань має велике значення. І незважаючи на значні досягнення нейронних мереж у розпізнаванні емоцій, моделюванні людської взаємодії, тут можна говорити про певні обмеження. Розуміння емоцій вимагає комплексної оцінки контексту, в якому вони виникають, а алгоритми штучного інтелекту можуть не помічати важливі контекстуальні сигнали, інтегрувати вербальні та невербальні сигнали, їм поки що важко вловити тонкий контекст емоцій. Також алгоритми штучного інтелекту чутливі до упереджень, наявних у даних, на яких вони навчаються. Система може ненавмисно зберегти ці дані, що призведе до дискримінаційної практики. У психології це може мати серйозні наслідки, оскільки упереджені системи можуть виставляти неправильні діагнози або давати неправильні рекомендації.

Також штучний інтелект у психології викликає етичні проблеми щодо конфіденційності, безпеки даних. Збір і аналіз персональних даних, таких як записи про емоції та психічне здоров'я може призвести до неправомірного використання.

Висновки:

Технології штучного інтелекту, які нещодавно стали доступні широкому колу користувачів значно змінюють та переформатовують суспільні процеси. Хоча вони ще в стадії розвитку, але вже зараз проявляють як позитивні так і негативні ефекти. Серед негативних ефектів — у користувачів спостерігаються емоції та психологічні стани, які виникають при реакції на щось нове і загрозливе, а також різного ступеня залежності від гаджетів та програмних продуктів, що використовують технології штучного інтелекту (асистенти, помічники). Також поглиблюються симптоми соціального дистанціювання та втечі від реальності.

Є певний вид спеціалізованих нейронних мереж, створених та натренованих на зміну поведінки людини. Експерименти показують, що вони можуть працювати ефективно і досягати результатів. Дані технології є еволюційним продовженням вже існуючих алгоритмів, направлених на стимулювання користувачів до бажаних дій, перш за все у галузі маркетингу. Але це тільки початок — і в майбутньому багато програмних продуктів будуть містити елементи ШІ, одним із задач якого буде зміна поведінки людини. У цьому випадку важливим стає регулювання і контроль, щоб запобігти шкідливим чи злочинним намірам.

Але разом з тим — технології ШІ можуть допомогти у боротьбі з психічними захворюваннями, завдяки здатності опрацьовувати великі обсяги даних та знаходити неочевидні закономірності, вони допомагають спеціалістам у прийнятті рішень щодо діагностування та лікування на основі даних пацієнтів.

Література

1. Banafa A., Psychological Impacts of Using AI [Електронний ресурс] / URL: https://www.bbvaopenmind.com/en/technology/digital-world/psychological-impacts-of-using-ai/ (дата звернення 10.11.2023)

2. Rachana X., Can Artificial Intelligence Influence Human Behavior? [Електронний ресурс] / URL: https://itmunch.com/how-artificial-intelligence-influences-behavior/ (дата звернення 10.11.2023)

3. Rosenfeld A., Benrimoh D. (2019) Big Data Analytics and AI in Mental Healthcare / arXiv preprint / arXiv:1903.12071v1 / [Електронний ресурс] URL: https://arxiv.org/abs/1903.12071

4. Tshepo C. N. Artificial Intelligence in Medical Sciences and Psychology: With Application of Machine Language, Computer Vision, and NLP Techniques. Apress, 2022, 185 c.

5. Kadia K., Role of Artificial Intelligence in Psychology [Електронний ресурс] / URL: https://acit-science.com/role-of-artificial-intelligence-in-psychology/ (дата звернення 11.11.2023

УДК 004.65

ЗАСТОСУВАННЯ ДОСЛІДНИЦЬКОГО АНАЛІЗУ ДАНИХ ПРИ РОБОТІ З НЕСТРУКТУРОВАНИМИ ДАНИМИ

Стасьо Олег, Бурак Назарій
Львівський державний університет безпеки життєдіяльності, м. Львів

Аналіз даних за допомогою ймовірнісно-статистичні методів вважається одним з найкращих та найнадійніших підходів для отримання достовірної інформації, прогнозування та пошуку закономірностей у великих об'ємах даних. Однак, більшість таких методів потребують чіткої структури даних, що накладає певні обмеження при роботі з неструктурованими даними. Проаналізовано особливості використання дослідницького методу аналізу даних при дослідженні інформації змінної структури.

Ключові слова: статистика, великі дані, методи, неструктуровані дані

Data analysis using probabilistic statistical methods is considered one of the best and most reliable approaches for obtaining reliable information, forecasting and finding patterns in large volumes of data. But, most of these methods require a clear data structure, which imposes certain limitations when working with unstructured data. The peculiarities of using the research method of data analysis in the study of variable structure information are analyzed..

Keywords: statistics, big data, methods, unstructured data

Статистика відіграє одну із ключових ролей в отриманні значущої інформації зі складних наборів даних. Вона полегшує формування висновків на основі аналізу великих даних. Постійний ріст кількості даних та різноманіття їх структури потребують нових та потужних інструментів і методологій, які б забезпечували б оптимальну швидкість та якість роботи під час виконання точного аналізу. Правильне уявлення про закономірності, тенденції, прогнози та прийняття рішень, статистичні дані для науки про дані є важливими для перевірки гіпотез, кількісного визначення невизначеностей і сприяють стабільності та надійності аналізу.

Переважна більшість даних, які генеруються в реальному світі, є неструктурованими і є життєво важливими для подальшого розуміння світу. Аналіз структурованих даних забезпечує можливість дізнатися, що відбувається, натомість неструктуровані дані можуть виявити першопричини виникнення цих подій. Оскільки неструктуровані дані не вписуються в структуру рядків і стовпців таблиці даних, це унеможливлює використання стандартних чисельних або статистичних методів аналізу для їх обробки. Це формує набір проблем, пов'язаних з визначенням закономірностей, тенденцій і значень у неструктурованих даних.

Перш ніж застосовувати методи аналізу неструктурованих даних, необхідно виконати підготовчі етапи, зокрема попередню обробку даних та зробити їх придатними для пошуку корисної інформації. Також важливо вибрати правильні та ефективні методи, залежно від мети аналізу неструктурованих даних та глибини видобутку корисних даних.

Одним із таких методів, які використовують для аналізу неструктурованих даних є ймовірнісно-статистичний, зокрема дослідницький аналіз даних.

Дослідницький аналіз даних (exploratory data analysis, EDA) — це набір початкових досліджень, які проводяться для визначення основних характеристик даних. Це робиться за допомогою зведеної статистики та графіки.

Застосування дослідницьких інструментів та методів аналізу даних у поєднанні з методами візуалізації даних формують ефективний пакет засобів для визначення основних характеристик наборів даних.

Методи дослідницького аналізу даних (далі – EDA) дозволяють ефективно маніпулювати джерелами даних, дозволяючи знаходити потрібні відповіді, виявляючи моделі даних, аномалії, перевіряти припущення або гіпотезу. Дослідницький аналіз даних може допомогти виявити очевидні помилки, виявити викиди в наборах даних, зрозуміти зв’язки, виявити важливі фактори, знайти закономірності в даних і надати нові ідеї.

Розроблений у 1970-х роках американським статистиком Джоном Тьюкі, відомим своїми методами прямокутних графіків і алгоритмом швидкого перетворення Фур’є, EDA продовжує знаходити свою актуальність навіть сьогодні в галузі статистичного аналізу. Це дозволяє фахівцям з обробки даних отримувати релевантні та достовірні результати, які використовуються при керуванні бажаними бізнес-цілями.

Існує чотири дослідницькі методи аналізу даних, зокрема:

Одновимірний неграфічний. Це найпростіший тип EDA, який застосовують при обробці даним із мінімальним набором змінних - однією змінною. У даному методів опрацьовуються неструктуровані дані без врахування зв'язків.

Одновимірний графічний. Неграфічні методи не представляють повної картини даних. Тому для комплексного EDA при роботі з масивами даних використовують графічні методи, такі як діаграми “стовбур-листя”(альтернативою лінійній діаграмі для отримання картини розподілу даних, коли дані можуть бути представлені у вигляді цілих чисел), коробкові графіки(візуалізовують розподіл даних із більш детальнішою інформацією: чітко показує викиди, максимум, мінімум, квартиль тощо) та гістограми.

Багатовимірний неграфічний. Багатовимірні дані складаються з кількох змінних. Неграфічні багатовимірні методи EDA ілюструють зв’язки між 2 або більше змінними даних за допомогою статистики або перехресної таблиці, що формує уявлення про структуру досліджуваних даних.

Багатовимірний графічний. Цей метод EDA використовує графіку для відображення зв'язків між 2 або більше наборами даних. ДО набору візуальних інструментів представлення зв'язків досліджуваних даних використовується стовпчасті діаграми, теплові карти, бульбашкові, циклічні, багатовимірні та діаграми розсіювання. Даний метод забезпечує повний та точний аналіз неструктурованих даних та дозволяє побудувати зрозумілу та придатну до інтеграції в інформаційні системи модель даних.

У результаті проведеного аналізу розглянуто ймовірнісно-статистичні методи аналізу неструктурованих даних, зокрема дослідницький аналіз даних та його підвиди. Застосування даних методів дозволить виконати попередній аналіз неструктурованих даних для визначення внутрішніх зв'язків та побудови моделі даних для подальшого видобутку корисної інформації. Інтеграція машинного навчання та штучного інтелекту в процес перетворення неструктурованих даних в структуровані з використанням розглянутих методів дозволить ефективно використовувати сучасні потужності обчислювальної техніки.

Література

1. Kushnir O. K., Chaplinsky V. R. Statistical Methods for Big Data Analysis, 2023. [Електронний ресурс]. – Доступний з : https://doi.org/10.31521/modecon.V39(2023)-11

2. Стасьо О.Р. Бурак Н.Є. Методи інтелектуального аналізу даних. Achievements of 21st Century Scientific Community: збірних тез доповідей I Міжнародної науково-практичної інтернет-конференції, 14-15 вересня 2023 року. – Міжнародний електронний науково-практичний журнал «WayScience». – С.426-429

3. Unstructured Data Analysis Techniques, [Електронний ресурс]. – Доступний з https://www.mongodb.com/unstructured-data/analysis

4. Statistics for Data Science: A Comprehensive Guide. [Електронний ресурс]. – Доступний з https://www.simplilearn.com/statistics-for-data-science-article

5. Exploratory Data Analysis Techniques for Unstructured Data. [Електронний ресурс]. – Доступний з https://www.kdnuggets.com/2023/05/exploratory-data-analysis-techniques-unstructured-data.html

6. Рогушина Ю. В. Засоби та методи аналізу неструктурованих даних. Проблеми програмування. 2019. № 1. С. 57–77. [Електронний ресурс]. – Доступний з http://pp.isofts.kiev.ua/ojs1/article/view/348/3 46

7. Khlevnoi, O., Burak, N., Borzov, Y., Raita, D. (2023). Neural Network Analysis of Evacuation Flows According to Video Surveillance Cameras. In: Babichev, S., Lytvynenko, V. (eds) Lecture Notes in Data Engineering, Computational Intelligence, and Decision Making. ISDMCI 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 149. Springer, Cham. https://doi.org/10.1007/978-3-031-16203-9_35

УДК 351.861

МАТЕМАТИЧНА МОДЕЛЬ ГУМАНІТАРНОГО РОЗМІНУВАННЯ ЯК ПРОЦЕСУ ФУНКЦІОНУВАННЯ ЕРГАТИЧНОЇ СИСТЕМИ «САПЕР ДСНС – ОБЛАДНАННЯ ТА ЗАСОБИ ЗАХИСТУ – НАВКОЛИШНЄ СЕРЕДОВИЩЕ»

Степанчук Сергій, Соловйов Павло, Стрілець Віктор
Національний університет цивільного захисту України,
ГУ ДСНС України в Херсонській області

Анотація. Проведення гуманітарного розмінування ускладнюється невідповідністю існуючого обладнання сучасним завданням. Показано, що наявність багатофакторних закономірностей оперативної діяльності саперів ДСНС дозволить обґрунтувати пропозиції щодо підвищення ефективності проведення гуманітарного розмінування. Відмічено, що для цього необхідно розробити математичну модель гуманітарного розмінування у загальному вигляді.

Ключові слова. Гуманітарне розмінування, математична модель, ергатична система

Abstract. Carrying out humanitarian demining is complicated by the inadequacy of existing equipment to modern tasks. It is shown that the presence of multifactorial regularities in the operational activity of sappers of the State Emergency Service will allow to substantiate proposals for improving the efficiency of humanitarian demining. It was noted that for this it is necessary to develop a mathematical model of humanitarian demining in general.

Key words. Humanitarian demining, mathematical model, ergatic system

Показано, що уявлення процесу проведення гуманітарного розмінування у вигляді функціонування системи функціонування системи «сапер ДСНС – обладнання та засоби захисту – навколишнє середовище» дозволяє отримати математичну модель гуманітарного розмінування у вигляді відповідної упорядкованої множини. В цій системі в якості вихідних даних присутні показники, що характеризують безпосередньо особовий склад оперативного розрахунку, обладнання та засоби захисту, умови проведення гуманітарного розмінування.

Умови, при яких процес гуманітарного розмінування представляється як ергатична система, дозволяє його представити у вигляді функціоналу

$$Y^* = F^*(X), \qquad (1)$$

де Y^* – сукупність показників ефективності; X – надмножина характеристик функціонування системи.

Даний функціонал може бути розглянуто як сукупність однофакторних моделей

$$y = f_i(x_i), \tag{2}$$

де y – конкретний показник ефективності; x_i – характеристика *i*-го фактора при незмінності (стабілізації) всіх інших факторах.

Це дозволяє перейти до ранжирування вагомих коефіцієнтів в однофакторних моделях

$$\left(x^{(1)}_{\min,\,0,(\max)} \geq x^{(2)}_{\min,\,0,(\max)} \geq \ldots \geq x^{(n)}_{\min\,,0,(\max)}\right) = \operatorname{rang}\left\{\begin{vmatrix} b_{y_{\min,\,0,(\max)}(x_1)} \\ b_{y_{\min,\,0,(\max)}(x_2)} \\ \ldots \\ b_{y_{\min,\,0,(\max)}(x_n)} \end{vmatrix}\right\}. \tag{3}$$

Тоді експертні оцінки і вибір оперативно-технічних рекомендацій можна описати як

$$G_{k'} = F_{k'}(X - \Delta X,\ T). \tag{4}$$

В результаті шукана математична представлена у вигляді системи рівнянь (1), (2), (3) та (4).

УДК004.032.26

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ПОКРАЩЕННЯ ПРОГНОЗУВАННЯ ГЕОМАГНІТИХ БУР

Ткаченко Роман, Панченко Сніжана, Гумен Олена
Національний технічний університет України "КПІ ім. Ігоря Сікорського"

Анотація. Використання методів машинного навчання для прогнозування геомагнітних бур стає актуальним в контексті їхнього потенційно негативного впливу на технічні системи. У дослідженні аналізується взаємозв'язок між магнітним полем та планетарним індексом Kp. Використовуючи методи машинного навчання, такі як регресія, та дані супутника DSCOVR, вивчаються можливості поліпшення точності прогнозів та визначаються фактори, що впливають на геомагнітні умови. Результати можуть мати практичне застосування для покращення алгоритмів прогнозування з метою захисту технічних систем від впливу геомагнітних збурень.

Ключові слова. Прогнозування геомагнітних бур, машинне навчання, планетарний індекс Kp.

Abstract. The use of machine learning methods for forecasting geomagnetic storms becomes relevant in the context of their negative impact on technical systems. The study analyzes the relationship between the magnetic field and the planetary index Kp. Using machine learning techniques, such as regression, and the DSCOVR satellite, opportunities to improve forecast accuracy are explored and factors influencing geomagnetic conditions are developed. The results can have practical applications for improving forecasting algorithms using the protection of technical systems against the influence of geomagnetic storms.

Keywords. Geomagnetic storm forecasting, machine learning, planetary index Kp.

Вступ. Геомагнітні бурі, спричинені змінами в сонячній активності, мають потенційно значущий вплив на технічні системи та людей, як у космосі, так і на Землі. Їхні наслідки охоплюють від перерв у роботі супутникових систем до проблем у роботі електроенергетичних мереж. Для попередження та зменшення можливих ризиків виникає потреба у точних та передбачуваних методах прогнозування геомагнітних умов.

Одним із ключових індикаторів геомагнітної активності є планетарний індекс Kp, який характеризує силу геомагнітного поля на північному та південному полюсах. Цей індекс визначається на основі спостережень геомагнітних обсерваторій та відображає загальний стан магнітосфери [1].

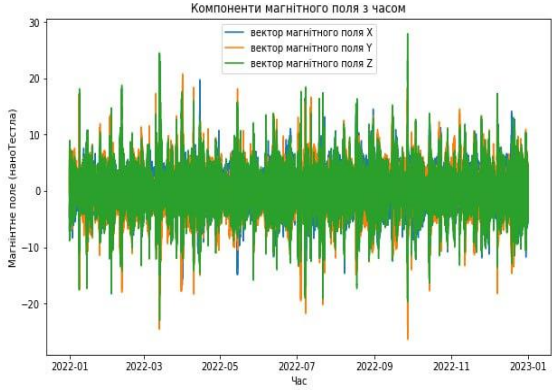
Методологія. У цьому контексті використання методів машинного навчання набуває обґрунтування, оскільки вони дозволяють аналізувати великі обсяги даних та виявляти складні залежності між показниками сонячної

та геомагнітної активності. В дослідженні ми розглядаємо використання методів машинного навчання з метою поліпшення алгоритмів прогнозування геомагнітних бур на основі аналізу взаємозв'язку між магнітним полем та планетарним індексом Kp. Використовуючи статистичні методи та моделі регресії, ми досліджуємо можливості покращення точності прогнозування та розглядаємо фактори, що впливають на геомагнітні умови

Дані та набори вимірювання. Для ефективного використання машинного навчання необхідно правильно обробити та підготувати вихідні дані. У нашому випадку використовуються два основних джерела даних: база даних планетарного індекса з Німецького дослідницького центру геонаук GFZ та набір даних магнітометра PlasMag, супутника DSCOVR [2]. Вимірювання інструментального комплексу DSCOVR PlasMAG містять значення даних, зареєстрованого сонячному вітру поблизу точки Лагранжа L1 Земля-Сонце, де кожен файл відповідає одному року вимірювань. Самі вимірювання були сконденсовані та децимовані до каденції одного набору вимірювань на хвилину. Кожен рядок: дата та час (UTC), три компоненти магнітного поля (нТл) у системі GSE. Та п'ятдесят значень, що представляють "сирий" спектр вимірювань з плазмового детектора чашки Фарадея. Кожне значення відповідає потоку, або силі потоку, сонячного вітру в певному діапазоні енергій. Ці числа не калібруються і не перетворюються - це безрозмірні числа, закодовані в комп'ютері приладу [3].

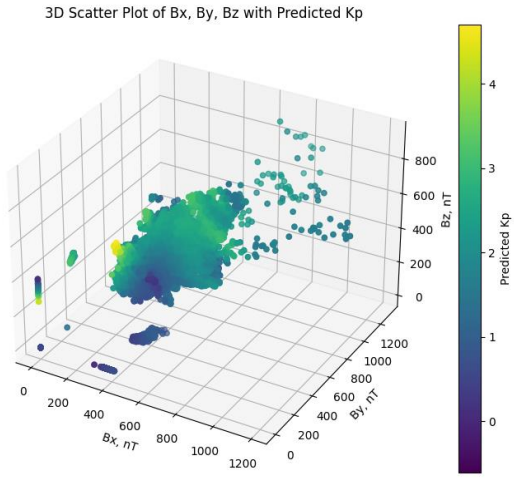
Оскільки детектори PlasMAG не збирають дані весь час, а чашка Фарадея не проводить вимірювання по всьому діапазону щохвилини - деякі дані можуть бути відсутні.

Моделювання та тренування. Для забезпечення взаємної сумісності даних варто зробити об'єднання даних по часу та окремо визначити та виділити значення планетарного індексу Kp та векторів магнітного поля (Bx, By, Bz) з об'єднаних даних, що надалі знайти кореляцію та спробувати передбачити Kp на кілька часових інтервалів наперед.



Для розв'язання завдання прогнозування ми обрали модель лінійної регресії, що зумовлене природою наших даних, та дозволяє визначити лінійну залежність між векторами магнітного поля та планетарним індексом.

Для тренування моделі варто використовувати частину даних: 80% даних використовується як навчальна вибірка, а 20% - для валідації.



Для оцінки метрик використовується, зазвичай, середньоквадратична похибка та коефіцієнт кореляції Пірсона, оскільки ця метрика дозволяє виміряти лінійну залежність між прогнозованими та фактичними значеннями планетарного індексу Kp та векторами магнітного поля. Коефіцієнт кореляції Пірсона між прогнозованими та фактичними значеннями Kp становив приблизно 0,603, що вказувало на досить велику позитивну кореляцію між планетарним індексом Kp та вектором магнітного поля Bz.

Висновки. Існуюча модель прогнозування геомагнітних бур за допомогою машинного навчання становить лише початок у розвитку більш точних та ефективних методів передбачення космічної погоди. Для забезпечення точних та надійних прогнозів геомагнітних бур використання лише векторів магнітного поля та планетарного індексу може бути недостатнім, саме тому додавання додаткових джерел інформації забезпечить більш повний та точний прогноз геомагнітних бур, що є критичним у контексті прогнозування космічної погоди.

Література

1. Bartels, J., Heck, N. H., & Johnston, H. F. (1939). Terrestrial Magnetism and Atmospheric Electricity, 44(4), 411–454. doi:10.1029/te044i004p00411.

2. NOAA Space Weather Prediction Center (2016): (2016). Deep Space Climate Observatory (DSCOVR). Retrieved from https://www.ncei.noaa.gov/access/metadata/landing-page/bin/iso?id=gov.noaa.ngdc.stp.swx%3Asatellite-systems _dscovr.

3. Shprits, Y. Y., Vasile, R., & Zhelavskaya, I. S. (2019). Space Weather, 17(8), 1219–1229. doi:10.1029/2018sw002141.

УДК 377:37.09:004

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ТРИВИМІРНОГО МОДЕЛЮВАННЯ В ПРОЦЕС ПІДГОТОВКИ КВАЛІФІКОВАНИХ РОБІТНИКІВ ПРИ ВИВЧЕННІ СПЕЦІАЛЬНИХ ПРЕДМЕТІВ ІЗ ЗАСТОСУВАННЯМ СУЧАСНИХ ТЕХНІЧНИХ ЗАСОБІВ НАВЧАННЯ

Ткаченко Руслан, Буравицький Владислав
Вище професійне училище Львівського державного університету безпеки життєдіяльності (м. Вінниця)

Анотація. У тезах розглянуто втілення новітніх інноваційних тривимірних технологій для популяризації спеціальних предметів у закладі освіти з метою здійснення переходу від книжкового до електронного контенту та підвищення ефективності освітнього процесу і рівня позитивної мотивації здобувачів освіти до опанування навчальним матеріалом.

Ключові слова: тривимірні технології, програмний комплекс, 3D моделювання, вузли захисних дихальних апаратів.

Abstract. The article deals with the implementation of the latest innovative three-dimensional technologies for the promotion of special subjects in vocational training establishments in order to make the transition from book to electronic content and increase the efficiency of the educational process and the level of positive motivation of the learners to master the material.

Key words: three-dimensional technologies, software complex, 3D modeling, nodes of respiratory protective devices.

Інноваційні технології швидкими темпами розвиваються в усіх галузях нашого життя. У зв'язку з цим у закладі освіти виникає нагальна потреба використання комп'ютерної техніки під час вивчення широкого спектру навчальних предметів при підготовці кваліфікованих робітників. Адже щоденно змінюється ситуація в світі, законодавство, природа, техніка. Інформація, подана в підручнику, перетворюється в застарілу ще під час видання підручника. Вивчення окремих предметів чи окремих тем з використанням інноваційних технологій, комп'ютерної техніки та найсвіжішої інформації, взятої з мережі Internet, - один із способів оптимізації та урізноманітнення освітнього процесу.

Ідея втілення інформаційно-комунікаційних технологій у навчання передбачає досягнення високоякісної освіти, тобто освіти конкурентноздатної, спроможної забезпечити кожній людині умови для самостійного досягнення тієї чи іншої цілі, творчого самоутвердження у різних соціальних сферах.

Нові інноваційні та інформаційні технології наприкінці XXI століття стали не тільки головною рушійною силою прогресу, засобом спілкування між державами, компаніями, закладами освіти, новою формою торгівлі, але й потужним засобом навчання.

Можна із впевненістю сказати, що комп'ютерні технології, які використовуються під час занять, дозволяють:

- за мінімум часу на уроці донести до здобувачів освіти більший обсяг навчального матеріалу, ніж під час роботи з підручником,
- своєчасно поповнювати теоретичні відомості новими фактами та подіями.

Крім цього, завдяки використанню інноваційних комп'ютерних технологій на заняттях можна значно розширити коло навчальних завдань, включаючи в освітній процес завдання нового типу.

Однією із інноваційних комп'ютерних технологій є застосування тривимірного моделювання для розробки деталей та вузлів захисних дихальних апаратів на стисненому повітрі [1, с. 32].

Вказані технології у Вищому професійному училищі Львівського державного університету безпеки життєдіяльності (м. Вінниця) почали впроваджувати з метою підвищення якісної успішності здобувачів освіти з предмета «Засоби індивідуального захисту органів дихання» та кращого розуміння будови і принципу роботи вузлів захисних дихальних апаратів на стисненому повітрі, так як відсутня можливість створення макетів деталей в розрізі.

Безпосередньо була вивчена програма тривимірного моделювання SolidWorks.

SolidWorks (Солідворкс) - програмний комплекс для автоматизації робіт промислового підприємства на етапах конструкторської та технологічної підготовки виробництва, який забезпечує розробку виробів будь-якого ступеня складності і призначення [2]. Працює в середовищі Microsoft Windows.

Solid Works вирішує наступні завдання:

- 3D проєктування виробів (деталей і зборок) будь-якого ступеня складності з урахуванням специфіки виготовлення;
- створення конструкторської документації відповідно до ДСТУ;
- розробка промислового дизайну;
- формування реверсного інжинірингу;
- проєктування комунікацій (електроджгутів, трубопроводів тощо);
- інженерний аналіз (міцність, стійкість, теплопередача, частотний аналіз, динаміка механізмів, газо-гідродинаміка, оптика і світлотехніка, електромагнітні розрахунки, аналіз розмірних ланцюгів і ін.);
- експрес-аналіз технологічності на етапі проєктування;
- аналіз технологічності конструкції виробу та ін.

Насамперед програма дозволяє створити деталь у форматі 3D, провести розріз у потрібній площині та зробити анімацію щодо принципу її роботи (рис. 1, 2, 3).

а) **б)**

Рисунок 1 – Редуктор захисного дихального апарата виробництва фірми MSA:
а) загальний вигляд редуктора, б) редуктор у розрізі

а) **б)**

Рисунок 2 – Запірний вентиль захисного дихального апарата виробництва фірми MSA:
а) запірний вентиль у розрізі, б) складові частини запірного вентиля

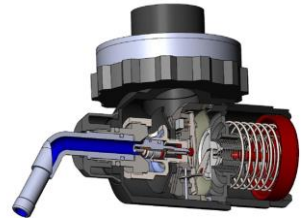


Рисунок 3 – Легеневий автомат виробництва фірми MSA у розрізі

Через відсутність достатньої кількості натурних зразків захисних дихальних апаратів закордонного виробництва та можливості їх розборки, в училищі програма Solid Works особливо широко використовується під час прове-

дення теоретичних і практичних занять з предмета «Експлуатація засобів індивідуального захисту органів дихання» навчального плану підготовки кваліфікованого робітника за професією 5169 «Майстер з обслуговування засобів індивідуального захисту органів дихання та компресорного обладнання».

Роботу з програмою Solid Works розпочато із розробки усіх вузлів апарата виробництва фірми MSA у форматі 3D. Потім результати сформовано у статичний технологічний альбом апарата (рис. 4), примірник якого видається кожному здобувачу освіти під час вивчення нового матеріалу. Здобувач освіти має можливість ознайомитися з будовою, принципом роботи, можливими несправностями деталей захисного дихального апарата та виробити шляхи їх усунення.

Рисунок 4 – Технологічний альбом вузлів ЗДА на стисненому повітрі фірми MSA

У процесі проведення занять викладач, крім статичних зображень у технологічному альбомі, повсякчас звертається до динамічних розробок програмного комплексу 3-D проєктування, що значно полегшує процес пояснення нового навчального матеріалу та залучає до активної роботи здобувачів освіти. По закінченню заняття майбутні робітники мають змогу виконати блог-квест з цієї теми (рис. 5). Здобувачі освіти зацікавляться навчальним матеріалом, оскільки він подається новими для них засобами, що і забезпечує кращу концентрацію уваги та мотивацію, а отже більш ефективне його засвоєння.

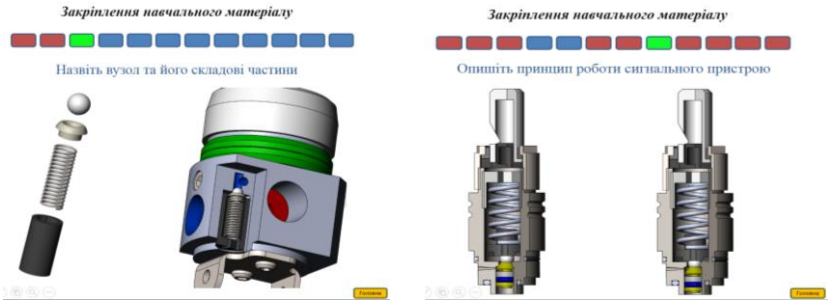


Рисунок 5 – Блог-квест з теми: «Призначення, будова, основні технічні характеристики та принцип роботи захисного дихального апарата виробництва фірми MSA»

Крім цього, використовуючи програмний комплекс 3D проєктування, можна продемонструвати спочатку загальний вигляд захисного дихального апарата (рис. 6), після цього у динаміці (кожна деталь від'єднується) показати будову кожного вузла та розкрити принцип його роботи (рис. 7).

Рисунок 6 – Загальний вигляд захисного дихального апарата ПОСТАУЭР-SL

а) **б)**

Рисунок 7 – Принцип роботи запірного вентиля захисного дихального апарата ПОСТАУЭР-SL:
а) в закритому положенні, б) у відкритому положенні

У такій послідовності демонструється будова та принцип роботи вузлів захисного дихального апарата. Така форма подачі навчального матеріалу дає можливість здобувачам освіти краще засвоїти будову та зрозуміти принцип роботи і можливі несправності вузлів.

Результати впровадження в освітній процес методу тривимірного моделювання показали, що цей метод у професійному навчанні здобувачів освіти, порівняно з традиційними, сприяє більш глибокому засвоєнню необхідного обсягу знань для виконання поставлених практичних завдань, мотивує до навчання та формує професійні компетентності, розвиває інтерес до предмета, сприяє розвитку логічного мислення, формуванню вмінь та навичок самостійного пошуку необхідної інформації та оцінювання власних знань на основі раціонального поєднання нових освітньо-інформаційних технологій і практичної діяльності, що в комплексі сприяє підвищенню якості знань, умінь та навичок здобувачів освіти у професійному навчанні. [1, с. 52]

Висновок. На сьогоднішній день існує різне за змістом і складністю програмне забезпечення, тому кожен викладач, враховуючи специфіку предмета, може підібрати для себе необхідну і зручну програму.

Впровадження тривимірних технологій не тільки позитивно впливає на процес засвоєння навчального матеріалу, а й сприяє інтересу та зацікавленості здобувачів освіти до предмета та до навчання в цілому.

Застосування інноваційних технологій дає новий імпульс системі професійного навчання, забезпечуючи доступ до гігантських обсягів інформації.

Нові апаратні та програмні засоби, розширюючи можливості комп'ютера, значно розширюють можливості ІКТ та їхнього використання у фаховій підготовці майбутніх працівників служби ДСНС.

Література

1. Гуревич Р. С. Інформаційно-комунікаційні технології в професійній освіті майбутніх фахівців / Р. С. Гуревич, М. Ю. Кадемія, М. М. Козяр ; за ред. член-кор. НАПН України Гуревича Р. С. – Львів : ЛДУ БЖД, 2012. – 380 с.

2. Програмне забезпечення як послуга [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/SolidWorks/ – Назва з екрана.

3. Козяр М. М. Інноваційні технології та кібернетичний підхід проектно-орієнтованого управління процесом підготовки професіонала-рятівника третього тисячоліття / М. М. Козяр, Ю. П. Рак // Пожежна безпека: Зб. наук. пр. – Львів: ЛДУБЖД, 2011. – №18. – С. 8-13.

УДК 351.861

ІНФОРМАЦІЙНА СИСТЕМА ОПЕРАТИВНОГО МОНІТОРИНГУ НАДЗВИЧАЙНИХ СИТУАЦІЙ У МІСТІ ЗА РЕЗУЛЬТАТАМИ АНАЛІЗУ АКУСТИЧНОГО ПРОСТОРУ

Усачов Дмитро
Національний університет цивільного захисту України, м. Харків, Україна

Анотація. Викладені основні принципи створення в моделі Safe city системи Smart city підсистеми контролю акустичного простору міста, з подальшим отриманням й обробкою інформації, а також прогнозування виникнення на території міста надзвичайних ситуацій (НС) різного характеру та розробкою ефективних управлінських антикризових рішень. Запропонований, для створення цієї підсистеми, системний підхід та принципи використання спектрального аналізу акустичного простору міста є основою для проведення подальших досліджень, спрямованих на розробку ефективної системи наземних автоматизованих пристроїв контролю акустичного простору та пасивної локації джерел небезпек.

Ключова слова: інформаційна система оперативного моніторингу надзвичайних ситуацій, контроль акустичного простору, спектральний аналіз, прийняття управлінських антикризових рішень.

Abstract. The main principles of creating a subsystem of the control of the acoustic space of the city in the Safe city model of the Smart city system, with further obtaining and processing of information, as well as forecasting the occurrence of emergency situations of various nature on the territory of the city and the development of effective management anti-crisis solutions are outlined. The proposed system approach and principles of using the spectral analysis of the acoustic space of the city for the creation of this subsystem are the basis for further research aimed at developing an effective system of ground-based automated devices for monitoring the acoustic space and passive location of sources of danger.

Keywords: information system for operational monitoring of emergency situations, acoustic space control, spectral analysis, making managerial anti-crisis decisions.

Сучасні міста, як елементи державної системи управління, є складними та розгалуженими системами з розподілом у просторі та часі параметрів життєдіяльності, які за чисельністю населення поділяються на невеликі, малі, середні, великі тощо, а також за характером спеціальних функцій на промислові, транспортні, наукові, історичні, багатогалузеві. Зворотнім боком даного процесу є те, що міста у процесі свого функціонування та розвитку створюють передумови для виникнення небезпек, що негативно впливають на стан природно-екологічного, економіко-технічного та соціально-політичного балансу як на території міста так і в регіоні, а також можуть завдати шкоди життєво важливим національним інтересам.

Один зі способів підвищення безпеки в сучасних містах – це створення ситуаційних центрів у рамках концепції Smart city [1, 2]. Ці центри

мають бути обладнані ефективною геоінформаційною системою оперативного моніторингу міської території з метою виявлення та ідентифікації джерел різноманітних небезпек.

В доповіді за стандартом IDEF0 розроблено структурно-функціональну модель стратегічного розвитку в загальній системі Smart city підсистеми Safe city, з урахуванням керуючих потоків нормативно-правової бази України та наявності в державі відповідних механізмів (ресурсів). В процесі моделювання показано, що процес реєстрації загроз для життєдіяльності міста включає організацію фінансового аудиту, моніторингу соціального стану та довкілля, відеоспостереження, радіаційного, хімічного та біологічного моніторингу, а також спектрального аналізу випромінювань від джерел небезпек.

Реалізація спектрального аналізу акустичного простору міста досягається тим, що безперервний та тривалий у реальному масштабі часу оперативний моніторинг за територією міста здійснюється за рахунок об'єднання у систему моніторингу наземних автоматизованих пристроїв контролю акустичного простору та пасивної локації джерел небезпек, а також отримання й обробки інформації від наземних пристроїв акустичного контролю ситуаційним центром, функціонування якого пов'язано з системою виконання антикризових рішень щодо запобігання, локалізації та ліквідації наслідків НС. Методи пасивної акустичної локації джерел небезпек мають свої специфічні особливості, а саме: в умовах відсутності інформації про тривалість акустичного випромінювання дальність до джерела випромінювання не можливо визначити за даними прийому тільки одного наземного засобу автоматизовано контролю акустичного простору. У зв'язку з цим, для визначення координат джерела небезпеки необхідно застосовувати комплекс двох або декількох рознесених у просторі засобів автоматизовано контролю акустичного простору, які з'єднані каналами зв'язку та утворюють комп'ютерну мережу; прийом прямого, а не відбитого сигналу, полегшує виявлення і вимір координат джерела небезпеки, але незнання форми сигналу та наявність інших джерел акустичного випромінювання ускладнює процес оперативного моніторингу за зоною НС; відсутність передавальних пристроїв при пасивній локації спрощує апаратуру, а також підвищує її енергозбереження та скритність. Функціональну схему цієї системи наземних стаціонарних засобів автоматизованого контролю акустичного простору, ситуаційного центру, підсистеми зв'язку та передачі телеметричної інформації, а також підсистеми виконання антикризових рішень щодо запобігання, локалізації та ліквідації наслідків НС, представлено на рис. 1.

Запропонований системний підхід та принципи використання спектрального аналізу акустичного простору міста служать основою для проведення подальших досліджень, спрямованих на створення ефективної системи наземних автоматизованих пристроїв контролю акустичного простору та пасивної локації джерел небезпеки. Ці дослідження передбачають

отримання та обробку інформації, а також прогнозування виникнення на території міста надзвичайних ситуацій різного характеру та розробку ефективних управлінських антикризових рішень.

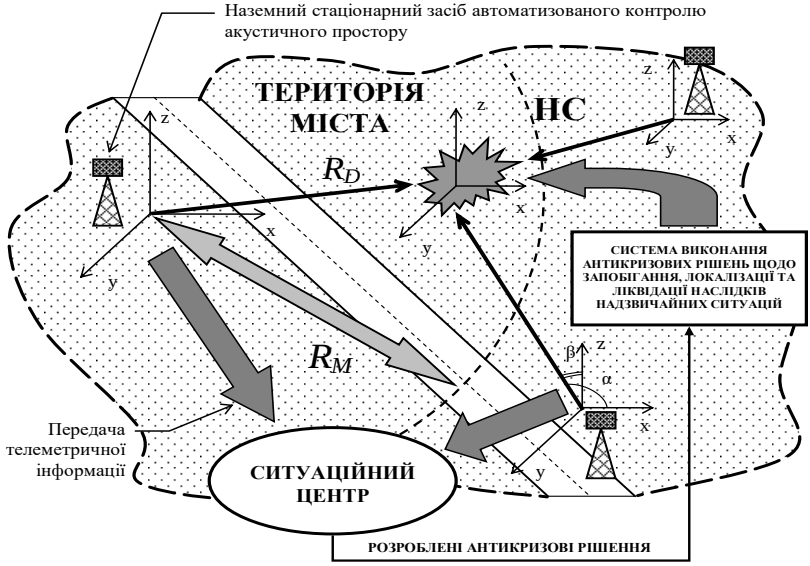


Рисунок 1 – Схема функціонування на території міста системи наземних стаціонарних засобів автоматизованого контролю акустичного простору, ситуаційного центру, підсистеми зв'язку та передачі телеметричної інформації, а також підсистеми виконання антикризових рішень щодо запобігання, локалізації та ліквідації наслідків НС різного характеру

Література

1. Smart Citi Ukraine: що це та як це працює в українських реаліях. [Електронний ресурс]. Режим доступу: https://visitukraine.today/uk/blog/2183/smart-city-ukraine-shho-ce-ta-yak-ce-pracuje-v-ukrainskix-realiyax

2. Тютюник В.В., Ященко О.А., Рубан І.В., Тютюник О.О. Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. Науковий журнал "Сучасні інформаційні технології у сфері безпеки та оборони". Київ. Національний університет оборони України імені Івана Черняховського. 2022. Вип. 1(43). С. 41–52. [Електронний ресурс]. Режим доступу: http://repositsc.nuczu.edu.ua/handle/123456789/15894

УДК 004.9

ЗАСТОСУВАННЯ ЧАТ-БОТІВ ДЛЯ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ КОРИСТУВАЧІВ У НАВЧАЛЬНОМУ ПРОЦЕСІ

Фіялковський В.І., Фрасоля Б.Р., Федорчук В.
Львівський національний університет природокористування, Львів

Abstract. The exploration of the research domain involved identifying potential project concepts, conducting a survey of analogous information systems, and conducting a comprehensive analysis of their functionality. In response to the defined objectives, a chat bot was developed to fulfil information help.

Keywords: Chat-bot, virtual communication, information system, messenger, information support, programming language

Чат-бот – це інформаційний помічник, який використовує віртуальну комунікацію з користувачами завдяки повідомленню і має велику кількість унікальних функцій [1]. Інформаційного чат-бота можна використати як для відправлення інформації, так і для її збору. На сьогодні такого типу месенджери користуються великою популярністю. Це пов'язано зі значним ростом мобільного Інтернету, що супроводжується покращенням швидкодії, низькою ціною і широким розповсюдженням смартфонів.

Розробка чат-боту дає змогу покращити взаємодію користувача з навчальним процесом в університеті. Бот є досить простий у використанні, що дає змогу користувачу легко почати з ним працювати. На сьогоднішній день люди користуються месенджерами для особистих потреб, таких як спілкування з іншими, пошук інформацій, або ж для забави. Завдяки чат-боту, університети можуть покращити доступ до інформації студенту або ж викладачу.

Для того, щоб зробити коректну та стабільну роботу інформаційної підтримки, необхідно буде вибрати, які саме інструменти взаємодії системи реалізації слід використати. Для виконання поставленої задачі щодо створення бота було використано мову програмування – Java. Інструментом управління та розуміння проєкту було обрано – Maven [2], комплексна модель для конфігурації системи – Spring Framework, хмарна платформа, яка дозволяє створити віддалене з'єднання користувачів без взаємодії хоста, доставляти інформацію, контролювати та масштабувати програми – Heroku [3] та база даних, яку надав сайт heroku PostgreSQL.

Наша задача полягала у тому щоб розробити чат-бота для інформаційної підтримки навчального процесу. Ми створили бота у месенджері, отримали ключ котрий дасть нам змогу почати працювати з ним та для його майбутніх модифікації.

Почали розробляти алгоритм за яким користувач буде отримувати потрібну йому інформацію. Зробили поділ потрібної інформації для користувача на розклад навчання та посилання на сайт, реквізити, опитування і конференції в zoom. Було створено окремий розділ куди користувач міг звернутись, щоб отримати відповідь на своє питання, також надавалась можливість користувачу запропонувати свою змінну в бота, а саме що корисного вони б хотіли бачити у ньому.

Боти telegram – це спеціальні облікові прилади, для налаштування яких не потрібен зв'язок з номером телефону.

Схема архітектури системи показана у рис. 1. та WBS діаграма на рисунку 2.

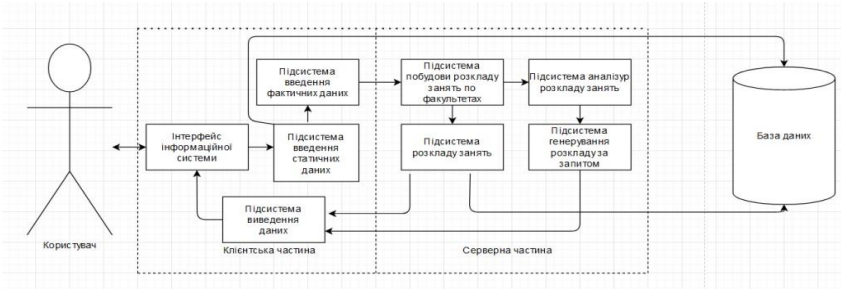


Рисунок 1 – Схема архітектури інформаційної системи

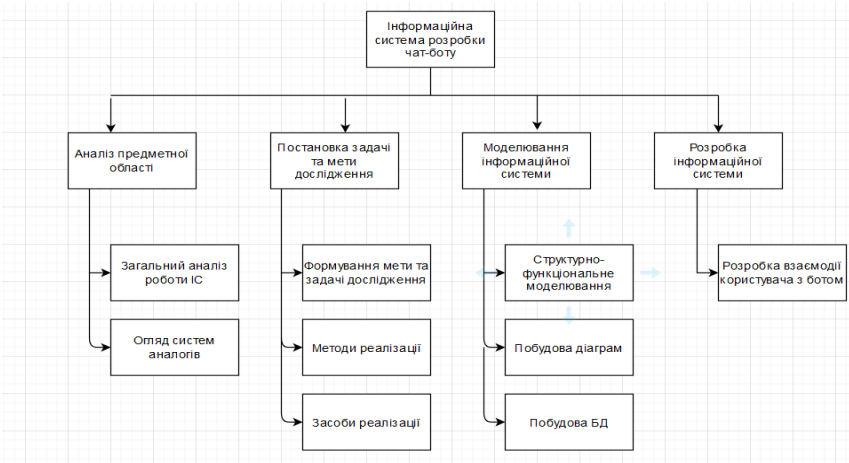


Рисунок 2 – WBS діаграма проекту інформаційної системи

Отже, в результаті виконання поставлених завдань розроблено чат-бот для інформаційної підтримки користувачів у навчальному процесі. Завдяки новим інноваційним підходам пов'язаним з використанням організації соціальних мереж в освітніх цілях, почалось стимулювання пізнавальної активності студентів і, як результат, підвищується якість освіти.

Література

1. Чат-бот.URL: https://sendpulse.ua/support/glossary/chatbot
2. Apache Maven. URL: https://uk.wikipedia.org/wiki/Apache_Maven
3. Heroku. URL: https://uk.wikipedia.org/wiki/Heroku
4. PostgreSQL. URL: https://uk.wikipedia.org/wiki/PostgreSQL

УДК: 004.932.2

ВИКОРИСТАННЯ МЕТОДІВ ГЛИБИННОГО НАВЧАННЯ ДЛЯ РОЗПІЗНАВАННЯ ОБЛИЧ

Ханін. Д.О., Отенко В.І.
Національний університет "Львівська політехніка", м. Львів

В роботі аналізуються традиційні та нейромережеві підходи покращення точності та ефективності систем розпізнавання облич, зокрема, методи глибинного навчання.

Ключові слова: розпізнавання облич, глибинне навчання, нейронні мережі, обробка зображень, біометрична аутентифікація.

This research examines conventional as well as neural network-based strategies to enhance the accuracy and efficiency of facial recognition systems, specifically emphasizing deep learning methodologies.

Keywords: facial recognition, deep learning, neural networks, image processing, biometric authentication.

Глибинне навчання радикально змінило підхід до систем розпізнавання облич, вносячи значні удосконалення у точності та надійності цих технологій. Використання нейронних мереж, здатних аналізувати величезні обсяги даних, дозволило виявляти складні взаємозв'язки та характеристики людського обличчя, які раніше були недоступні для класичних методів.

На відміну від традиційних алгоритмів, які базувалися на жорстко заданих правилах та ознаках, глибинне навчання дозволяє системам самостійно вчитися та адаптуватися. Наприклад, застосування конволюційних нейронних мереж (Convolutional Neural Networks, далі - CNN) [1] призвело до значного покращення в розпізнаванні облич у складних умовах, таких як зміна освітлення, положення, виразу обличчя або часткове його прикриття.

Технології розпізнавання облич значно еволюціонували протягом останніх десятиліть, переходячи від традиційних методів, що базуються на ручному визначенні ознак, до сучасних методів глибинного навчання, які використовують глибинні нейронні мережі, навчені на великих наборах даних.

Початкові алгоритми розпізнавання облич, які з'явилися на початку 70-х років, використовували прості зображення для опису геометрії облич. Ці методи працювали лише в обмежених умовах, проте демонстрували можливість використання комп'ютерів для автоматичного розпізнавання облич. Пізніше набули популярності методи статистичних підпросторів [2], такі як аналіз головних компонент (Principal Component Analysis), та лінійний дискримінантний аналіз (Linear Discriminant Analysis), які використовують увесь регіон обличчя як вхідні дані. Одночасно були розроблені локальні екстрактори ознак для опису текстури зображення в різних його локаціях, що дало змогу створити підходи, які полягають у порівнянні локальних ознак різних зображень облич.

Переваги класичних методів полягають у їхній простоті, швидкості обробки та ефективності в стандартних умовах. Проте, ці методи часто обмежені в своїй гнучкості та адаптивності, особливо у випадку різноманітності умов та особливостей облич. Такі методи мають проблеми з точністю в неконтрольованих середовищах, зокрема, через різноманітність облич в реальному житті, які включають різні положення голови, освітлення, вікові зміни та вирази обличчя.

Натомість, глибинне навчання використовує CNN та великі набори даних для вивчення оптимальних ознак, ефективних для репрезентації даних. Основною перевагою глибинного навчання є його здатність навчатися з великих наборів даних, які містять реальні варіації, що дозволяє досягнути високої точності розпізнавання. Це дає змогу перевершити традиційні підходи до розпізнавання облич, оскільки навчання здійснюється з наборів даних, які містять різноманітні зображення обличчя.

Компоненти системи розпізнавання облич включають їх виявлення, вирівнювання, репрезентацію та порівняння шаблонів [3]. Найважливішим компонентом є репрезентація облич, яка перетворює значення пікселів зображення у компактний та дискримінативний вектор ознак, також відомий як шаблон.

Переваги глибинного навчання включають його високу точність, гнучкість та здатність адаптуватися до нових умов. Глибинне навчання дозволяє системам ефективно справлятися з різноманітністю обличчя завдяки використанню великих наборів даних, які включають різні варіації облич.

Одним з ключових елементів глибинного навчання для розпізнавання облич є розвиток дискримінативних функцій втрати, які допомагають визначити, наскільки добре модель розпізнає різні обличчя. Ці функції включають Euclidean-distance-based Loss, Triplet loss [4] та їх різновиди, які сприяють точному відокремленню ознак різних облич у навчальних даних. Крім того, істотною є еволюція самої архітектури нейронних мереж, що забезпечує ще кращу адаптацію та вдосконалення у здатності розпізнавання в різних умовах.

Підхід до ідентифікації облич включає два основних процеси: верифікацію та ідентифікацію облич. Верифікація облич полягає в порівнянні двох облич для встановлення їхньої ідентичності, в той час як ідентифікація облич передбачає визначення конкретної особистості на основі зразка обличчя. Обидва ці процеси вимагають точного та надійного визначення унікальних характеристик обличчя.

Великомасштабні набори даних і стандартизовані протоколи оцінки також стають невід'ємною частиною процесу навчання та оцінки систем розпізнавання облич. Використання різноманітних і великих наборів даних дозволяє моделям глибинного навчання навчатися та адаптуватися до широкого спектру варіацій у зовнішності людей, що підвищує загальну точність і надійність системи розпізнавання облич [5].

Проблеми глибинного навчання в галузі ідентифікації обличчя стосуються точності, гнучкості та обробки великих наборів даних, а також забезпечення безпеки і конфіденційності інформації. Вирішення цих проблем вимагає подальших досліджень та розвитку технологій, спрямованих на підвищення ефективності систем ідентифікації облич.

Література

1. CNN Explainer: Learning Convolutional Neural Networks with Interactive Visualization, 2020, Zijie J. Wang, Robert Turko, Omar Shaikh, Haekyu Park, Nilaksh Das, Fred Hohman, Minsuk Kahng, and Duen Horng (Polo) Chau. URL: https://arxiv.org/pdf/2004.15004.pdf

2. Principal Component Analysis for Dimensionality Reduction, 2015, Funda Gunes. URL: https://blogs.sas.com/content/subconsciousmusings/2015/10/26/principal-component-analysis-for-dimensionality-reduction/

3. Face Recognition: From Traditional to Deep Learning Methods, 2018, Daniel Saez Trigueros, Li Meng, Margaret Hartnett. URL: https://arxiv.org/pdf/1811.00116.pdf

4. Self-restrained Triplet Loss for Accurate Masked Face Recognition, 2021, Fadi Boutros Naser Damer , Florian Kirchbuchner , Arjan Kuijper. URL: https://arxiv.org/pdf/2103.01716.pdf

5. Going Deeper Into Face Detection: A Survey, 2021, Shervin Minaee, Ping Luo, Zhe Lin, Kevin Bowyer. URL: https://arxiv.org/pdf/2103.14983.pdf

УДК 371.3

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ДОПОВНЕНОЇ РЕАЛЬНОСТІ ДЛЯ ПРИЙНЯТТЯ РІШЕНЬ В СІЛЬСЬКОМУ ГОСПОДАРСТВІ

Цап Марта, Катанюк Іван
Львівський національний університет природокористування, м. Дубляни

Здійснено огляд основних видів смарт-технологій, які використовуються в сільському господарстві. Наведено приклади практичного застосування технології доповненої реальності для вирішення управлінських задач в аграрному секторі. Окреслено перспективи покращення процесу прийняття управлінських рішень з використанням технології доповненої реальності в рослинництві та тваринництві.

***Ключові слова**:* інформаційні технології, доповнена реальність, сільське господарство, прийняття управлінських рішень

An analysis of the fundamental types of smart technologies utilized in the field of agriculture has been conducted. Exemplars of the practical application of augmented reality technology for addressing managerial challenges in the agrarian sector are provided. The prospects for optimizing the managerial decision-making process through the utilization of augmented reality technology in both crop cultivation and animal husbandry have been delineated.

***Keywords**:* information technologies, augmented reality, agriculture, decision-making.

Розвиток інформаційних технологій останніми роками позитивно вплинув на діджиталізацію окремих галузей економіки, у т.ч. і сільське господарство. Сьогодні важко уявити будь-які технологічні процеси в потужних аграрних підприємствах, які не передбачають використання інформаційних технологій для збору даних, які надходять з датчиків сучасної сільськогосподарської техніки, дозволяючи здійснювати детальніший контроль за внесенням засобів захисту рослин, витратою паливо-мастильних матеріалів тощо. Звісно, не всі сільськогосподарські виробники в умовах викликів військового часу мають можливість оновлювати матеріально-технічну базу та впроваджувати смарт-технології у виробництві, однак світова практика показує, що частка виробників, які використовують сучасні інформаційні технології для ведення господарської діяльності та прийняття управлінських рішень, щороку лише зростає.

Сільське господарство є доволі технологічною галуззю, яка застосовує різноманітні смарт-технології в рослинництві, тваринництві, садівництві тощо та впроваджує системи точного землеробства. Експерти аграрного ринку виділяють такі напрямки застосування смарт-технологій (від слова та абревіатури SMART):

1. Для збору і аналізу інформації (GNSS, GIS, RS, Web, Big Data, Yield monitoring, Soil-test і т.д.).

2. Для управління і прийняття рішень (Crop-, Land-, Livestock-management).

3. Для виконання прийнятих рішень (Variable Rate Technology) [1].

Технологія доповненої реальності в окремих випадках може стати корисним доповненням до набору смарт-технологій, які мають перспективи використання в аграрній сфері.

Під доповненою реальністю переважно розуміють технологію, яка накладає створене комп'ютером зображення на реальний світ користувача, забезпечуючи таким чином відповідне зображення. Підвидом технології доповненої реальності може бути змішана реальність.

В умовах обмежених ресурсів, зростання цін на сортове насіння, засоби захисту рослин, паливо-мастильні матеріали, своєчасна діагностика хвороб рослин, виявлення шкідників та стану ґрунту дасть змогу точково і своєчасно реагувати на проблеми, що виникли та приймати ефективні рішення. Доповнена реальність не менш ефективна в управлінні процесами в тваринництві, адже може допомагати фермеру аналізувати стан тварин, їх хвороби, потреби в харчуванні та вигулі, виявляти проблемні місця.

Нові співробітники можуть проходити віртуальне навчання, відпрацьовувати певні сценарії використання сільськогосподарської техніки, дронів та іншого дороговартісного обладнання в ігровому режимі та тренувати свої навички, що дасть змогу зменшити втрати та показники травматизму, підвищити ефективність традиційного навчання.

У випадку інтеграції доповненої реальності з іншими смарт-технологіями, такими як дрони, сенсори, датчики ґрунту та метеодані про погоду, фермери можуть відстежувати свої посіви на відстані та збирати дані про врожайність. Отримані дані можна використовувати для більш точного прогнозування врожайності та допомоги фермерам у плануванні майбутніх урожаїв [2].

В таблиці 1 наведено основні напрями застосування доповненої реальності в діяльності аграрних підприємств.

Таблиця 1 – Застосування доповненої реальності в аграрній сфері*

Назва	Опис
Візуальний моніторинг ферм	За допомогою доповненої реальності фермери можуть візуалізувати ферму або поля на одній інформаційній панелі, контролювати загальну якість продукції.
Навчання персоналу	Доповнена реальність допоможе новим працівникам навчитися використовувати складну сільськогосподарську техніку або обладнання, мінімізуючи при цьому серйозні нещасні випадки.

Діагностика хвороб рослин, шкідників та стану ґрунту	Візуалізація стану посівів, шкідників та ґрунту в режимі реального часу дозволить майже миттєво ідентифікувати шкідників та формувати відповідні рекомендації щодо боротьби з ними, а також забезпечить оцінку якості земель.
Швидше прийняття рішень за рахунок кращого розуміння візуалізованих даних	Візуально відображені дані на екрані доповненої реальності набагато легше засвоюються, ніж ті самі дані, записані у паперовому звіті.

Джерело: узагальнено на основі даних [3-4]

Існує ряд моделей реалізації та застосування доповненої реальності в аграрному секторі, серед яких можна виділити форми оптичної та відео присутності, у т.ч. із використанням мобільних додатків відомих як Mobile Augmented Reality [5].

Незважаючи на існуючі перспективи застосування доповненої реальності в сільському господарстві, можна виділити чинники, які впливатимуть на ефективність використання цієї технології на практиці:

1) швидкість та якість інтернету;
2) наявність розвиненої інформаційної інфраструктури та технічного обладнання;
3) вартість закупівлі та обслуговування, потреба інтеграції в існуючі бізнес-процеси;
4) потреба у навчанні персоналу.

Доповнена реальність може стати одним із драйверів розвитку сільського господарства, виходячи із можливостей технології та її поєднання із іншими смарт-технологіями, у т.ч. і перспектив застосування генеративного штучного інтелекту для обробки даних та навчання.

Література

1. Смарт-технології в агроменеджменті [Електронний ресурс] – Режим доступу: https://blog.agrokebety.com/smart-tehnologii-v-agro-menedgmente-ua
2. Frąckiewicz M. Доповнена реальність у сільському господарстві: потенціал і виклики [Електронний ресурс] – Режим доступу: https://ts2.space/uk/
3. Augmented Reality (AR) in Agriculture [Електронний ресурс] – Режим доступу: http://sparkle-project.eu/augmented-reality-ar-in-agriculture/
4. Розумне сільське господарство готове до доповненої та віртуальної реальності [Електронний ресурс] – Режим доступу: https://agroreview.com/content/rozumne-silske-gospodarstvo-gotove-do-dopovnenoyi-ta-virtualnoyi-realnosti/
5. Hurst W., Frida Ruiz Mendoza F., Tekinerdogan B. Augmented Reality in Precision Farming: Concepts and Applications [Електронний ресурс] – Режим доступу: https://edepot.wur.nl/558608

УДК 637.5.02

АЛГОРИТМ ПОШУКУ ЗОБРАЖЕНЬ НА ОСНОВІ ХЕШУ, ЧУТЛИВОГО ДО ЛОКАЛЬНОСТІ, З ВИКОРИСТАННЯМ ЗГОРТКОВОЇ НЕЙРОННОЇ МЕРЕЖІ ТА МЕХАНІЗМУ УВАГИ

Черніков Д. В., Лясковська С. Є.
Національний університет «Львівська політехніка», Львів

У роботі розглядається задача підвищення швидкості пошуку зображень завдяки поєднанню згорткової нейронної мережі та механізму уваги. Мета роботи досягається за рахунок конвертації вхідного зображення у хеш і подальшій передачі цього хешу натренованій моделі, у яку інтегровано шар уважності. Модифікація полягає у використанні чутливості до локальності, що у моєму випадку означає пошук спільних рис зображень / класифікація, що забезпечує ефективність пошуку серед схожих зображень. Експиментальні дослідження показали, що в середньому швидкість обробки зображень алгоритмом зростає на 40%, якщо використовувати технологію механізму уваги.

Ключові слова: механізм уваги, класифікація, підвищення ефективності пошуку.

The paper considers the task of increasing the speed of image search through a combination of a convolutional neural network and an attention mechanism. The goal of the work is achieved by converting the input image into a hash and then transferring this hash to a trained model, into which a layer of mindfulness is integrated. The modification is to use locality sensitivity, which in my case means looking for common features of images / classification, which ensures the efficiency of searching among similar images. Experimental studies have shown that, on average, the speed of image processing by the algorithm increases by 40% if the technology of the attention mechanism is used.

Key words: attention mechanism, classification, search effectiveness improvement.

Сучасний розвиток глибокого навчання відкриває нові перспективи в аналізі та обробці зображень. Підходи глибокого навчання, такі як згорткові нейронні мережі (ЗНМ), стали потужним інструментом для вирішення завдань визначення образів, класифікації та виявлення зразків. Застосування ЗНМ дозволяє ефективно враховувати просторові залежності в зображеннях, особливо враховуючи їх успішність у визначенні локальних особливостей та взаємодій між елементами.

Ефективність глибокого навчання полягає в його здатності автоматично вивчати представленням даних автоматично. ЗНМ можуть ефективно визначати оптимальні риси для кожного завдання, роблячи їх гнучким та універсальним інструментом аналізу зображень. Це важливо в сучасному контексті, де великі обсяги візуальної інформації вимагають швидкої та точної обробки.

У сфері аналізу зображень механізми уваги стають важливим аспектом оптимізації процесу. Механізми уваги дозволяють системі приділяти більше уваги певним частинам зображення, поліпшуючи точність та швидкість обробки. Такий підхід знаходить своє застосування в областях, де важлива конкретна інформація та деталі як от для камер спостережень, які повинні розпізнати пожар[1].

Застосування глибокого навчання у візуальному аналізі розширює його застосування в різних галузях. Від розпізнавання облич, автоматичної класифікації зображень до робототехніки, ЗНМ та механізми уваги визначають нові стандарти технологічного прогресу.

При використанні глибокого навчання важливо враховувати етичні та безпекові аспекти. Автоматизація та швидка обробка великих обсягів інформації породжують питання про конфіденційність та можливість недобропорядного використання цих технологій.

Метою цієї роботи є підвищення швидкості та ефективності обробки зображень за рахунок використання чутливості до локальності та механізму уваги.

Я розглядав декілька моделей ЗГН, а саме: ResNet, VGG16 та xceptoin. Проте зупинився на VGG16, оскільки після експериментальних випробовувань, вона показала кращий час обробки. Чутливість до локальності розтлумачую як пошук схожості для відображення подібних елементів в одній базі даних з високою ймовірністю співпадінь. Тут чутливість працює шляхом хешування подібних вхідних елементів у хеш-контейнери, що робить ефективним пошук подібних елементів у цих сегментах. Тобто, якщо кортко, це можна описати як класифікацію. Щодо механізму уваги, то у моєму випадку його можна імплементувати як один з шарів у моделі VGG16, дозволяючи їй зосереджуватись на різних частинах вхідної послідовності під час обробки зображення. Важливо нагадати, що механізм вказує моделі, куди потрібно звернути увагу, а що можна взагалі пропустити як незначуще, що в теорії підвищує швидкість опрацювання зображень.

Для тренування моделі, було використано 1000 різних зображень з датасету, а далі натренована модель використовувалась для пошуку схожих зображень з використанням бази даних на 100000 зображень. Було проведено порівняння часу опрацювання матеріалу з та без механізмом уважності. Результати показані на рисунках 1 та 2, де IPS - images per second (зображення за секунду)

```
--------------------------------------
Результати пошуку без механізму уважності:
--------------------------------------
Початкова швидкість пошуку: 5 IPS.
Після створення хеш-кодів для перших 1000 зображень: 15 IPS.
Після стабілізації та кешування результатів: 30 IPS.
--------------------------------------
```

Рисунок 1 – Результати пошуку без механізму уважності

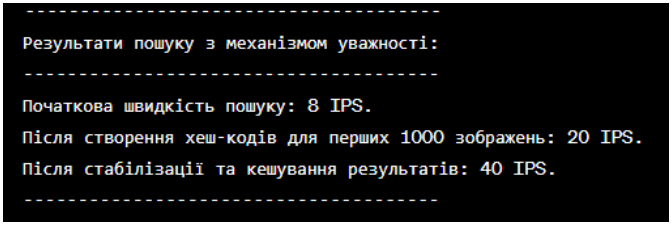


Рис. 2 Результати пошуку з механізмом уважності

Як видно з порівняння рисунків 1 та 2, алгоритм працює в середньому на 30-40% швидше з механізмом уважності, ніж без нього. Може здаватись, що це незначний результат, враховуючи що початкова обробка й так відбувається при показнику 5 зображень за секунду, а після стабілізації взагалі 30, проте треба враховувати, що база даних може мати мільйони зображень, і прискорення на 40% виглядає як успіх.

ВИСНОВКИ

У роботі розглядається задача з підвищення швидкості пошуку зображень за допомогою використання механізму уважності для моделі згорткової нейронної мережі. У підсумку, глибоке навчання відкриває нові горизонти у візуальному аналізі. І тому використання цих методів у реальному часі може забезпечити значні вигоди в широкому спектрі застосувань, від медичної діагностики до віртуальної реальності. Експериментальні дослідження показали, наскільки можна пришвидшити аналіз зображень за допомогою комбінації механізму уважності та чутливості до локальності.

Література

1. S Sarkar, AS Menon, T Gopalakrishnan, "Convolutional neural network (CNN-SA) based selective amplification model to enhance image quality for efficient fire detection" [Online]. Available: https://mecs-press.net/ijigsp/ijigsp-v13-n5/IJIGSP-V13-N5-5.pdf. [Accessed June 6, 2023].

УДК 004.652

СХОВИЩА ДАНИХ ЯК НАСТУПНИЙ ЕТАП РОЗВИТКУ БАЗ ДАНИХ

Чмир Тарас, Бурак Назарій
Львівський державний університет безпеки життєдіяльності

На сучасному рівні інформатизації суспільства, що керується даними, де інформація надходить із різних джерел з усього світу, сховища даних стали важливою опорою оперативного та ефективного управління. Вони формують спеціалізовані сховища для обробки постійно зростаючого обсягу даних, які часто надходять у неструктурованих форматах. Структуризація вхідної інформації оптимізує зберігання, пошук і систематичний аналіз даних, пропонуючи організаціям цінну інформацію.

Ключові слова: сховища даних, аналіз, моделі, озеро даних.

At the current level of IT impact on data-driven society, where information comes from various sources from all over the world, data warehouses have become an important pillar of operational and effective management. They form specialized repositories to handle ever-increasing volumes of data, often arriving in unstructured formats. The structuring of incoming information optimizes the storage, retrieval and systematic analysis of data, offering organizations valuable information.

Key words: data warehouses, analysis, models, data lakes.

Ідея сховища даних вперше виникла в середині 1980-х років з наміром забезпечити широкий аналіз даних і управлінську звітність. Сховище даних – це місце, де організовані дані зберігаються, перевіряються та витягуються. Ці дані можуть бути історичними або нещодавно згенерованими. Малі та середні підприємства зазвичай використовують хмарні служби для зберігання даних, тоді як великі організації та транснаціональні корпорації використовують сховища даних для керування великими обсягами даних. Щоб забезпечити можливість запитів і аналізу для прийняття рішень, Ральф Кімбол визначає сховище даних як систему, яка збирає, очищає, узгоджує та доставляє вихідні дані в сховище розмірних даних.

Окрім широкого використання в банківській справі, фінансах, споживчих товарах, роздрібній торгівлі та виробництві на основі попиту, сховища даних також набули популярності в некомерційних секторах, таких як охорона здоров'я, уряд, військові, освіта та дослідження. Сховище даних – це, як правило, спеціальна система баз даних лише для читання, яка об'єднує дані з кількох баз даних та інших джерел інформації.

Транзакційні бази даних зосереджені на відповідях на запитання типу «хто» та «що» та не дуже підходять для відповідей на запитання типу «що-якщо», «чому» та «що далі» через брак організації для аналітичної обробки.

Архітектура сховища даних описує компоненти сховища та спосіб їх поєднання. Сховища даних не зберігають неструктуровані дані. Натомість вони спочатку аналізують необроблені дані та використовують програмне забезпечення для перетворення їх на структуровану інформацію, що робить її легко доступною та зручною для використання. Дані надходять із різних каналів, перетворюються в проміжну зону, а потім інтегруються та зберігаються у сховищі виробничих даних для подальшого аналізу. Точність вилучення даних із багатьох джерел має вирішальне значення, оскільки можливі помилки та аномалії під час інтеграції різних наборів даних у сховище.

Однак, у час цифрового потоку даних, існуючі методи сховища даних не можуть впоратися зі складністю та аналізом процесів отримання значущої інформації. Тому потрібні інструменти для вилучення, очищення, інтеграції та завантаження даних.

Дані зберігаються та управляються в сховищі, яке надає засоби для багатовимірних візуалізацій даних для різних інструментів інтерфейсу користувача, таких як інструменти запитів, звітів, аналізатори та інструменти інтелектуального аналізу даних. Сучасні сховища даних оптимізовані для аналізу великих обсягів даних, а не швидкості виконання окремих транзакцій.

Сьогодні розрізняють три типи моделей сховищ даних: сховище корпоративних даних, вітрина даних та віртуальне сховище.

Сховище корпоративних даних(Enterprise Data Warehouse, EDW) — це реляційне сховище даних, яке містить бізнес-дані компанії, включно з інформацією про її клієнтів. EDW дозволяє аналізувати дані, які можуть надати корисну інформацію. Як і всі сховища даних, EDW збирає та агрегує дані з багатьох джерел і діє як сховище для більшості або всіх корпоративних даних, забезпечуючи широкий доступ і аналіз.

Вітрина даних — це підмножина сховища даних, орієнтована на певну бізнес-сферу, відділ або предметну область. Вітрини даних роблять певні дані доступними для визначених груп користувачів, щоб вони могли швидко отримати доступ до ключових відомостей, не витрачаючи час на пошук у загальному сховищі даних. Наприклад, багато компаній можуть мати вітрини даних, які обслуговують певні відділи компанії.

Віртуальне сховище або віртуальне сховище даних — це інший термін для обчислювальних кластерів, які наповнюють сучасне сховище даних, діючи як ресурс на вимогу. Віртуальні сховища часто збирають дані з різних джерел.

Майбутнє сховищ даних визначається постійними технологічними змінами та зміною вимог до даних. Сховища даних в основному зосереджені на структурованих даних. Однак значна тенденція передбачає інтеграцію та аналіз неструктурованих даних, що породило концепцію озер даних. Еволюція сховищ даних залежить від інтеграції озер даних із традиційними сховищами даних, створюючи надійну екосистему для керування та аналізу широ-

кого діапазону форматів даних. Хмарні рішення для сховищ даних стають доступнішими та економічно ефективнішими, а також забезпечують хорошу масштабованість, менші витрати на інфраструктуру та здатність обробляти величезні обсяги даних.

Сховища даних пропонують значні переваги. Вони допомагають організаціям, інтегруючи дані, проводячи ефективний аналіз і надаючи доступ до історичних даних. Ці сховища діють як центральний центр для структурованих даних, що дозволяє приймати обґрунтовані рішення. Оскільки дані продовжують розширюватися, вкрай важливо оцінити потреби в управлінні даними. Майбутнє рішення може полягати в гібридних підходах, що поєднують озера даних і сховища для кращої обробки даних.

Література

1. Kimball, R., & Casertam, J. (2004). The Data Warehouse ETL Toolkit

2. Зінов'єва І.С. Сучасні підходи до подальшої еволюції концепції баз даних / І.С. Зінов'єва // Scientific Publishing Center «Sci-conf. com. Ua». – 2019. – С. 34-44 [Електронний ресурс]. – Режим доступу : https://ir.kneu.edu.ua/bitstream/handle/2010/38140/Zin_2019_2.pdf?sequence=1.

3. Захарченко, Раїса & Захарченко, Леонід & Кірюшатова, Тетяна & Кибалко, Ігор. (2020). Дослідження методів збереження інформації у сховищах даних. Problems of information technologies. 54-68. 10.35546/2313-0687.2020.27.54-68.

4. Придатко О. В., Бурак Н. Є., Дзень В. Є., Кунинець М. С. Адаптивна інформаційно-довідкова система "UniBell" як складова частина проєкту "Smart-університет". Науковий вісник НЛТУ України. 2020, т. 30, № 5. С. 105–113

УДК 614.8:574.2

МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ ВИНИКНЕННЯ ЗАТОПЛЕННЯ ТЕРИТОРІЙ НА РІВНІ ОБ'ЄДНАНИХ ТЕРИТОРІАЛЬНИХ ГРОМАД

Шарко А.Є., Гаврись А.П.
Львівський державний університет безпеки життєдіяльності, м. Львів

В аналітичній доповіді національної ради з розвідки США «Глобальні тенденції 2030: альтернативні світи» [1] визначені потенційні небезпеки, які можуть спричинити максимальну руйнівну дію. Однією з головних загроз міжнародній безпеці називається зміна клімату.

Зміна клімату порушує економічний розвиток країн і має абсолютно вимірювані фінансові наслідки, які з кожним роком тільки зростають. З іншого боку очевидно, що сьогодні росте усвідомлення того, що способи вирішення проблеми і виходу з ситуації існують не тільки на рівні держави чи області, а й на місцевому рівні, а саме рівні об'єднаних територіальних громад (ОТГ). Проте процес децентралізації в Україні розпочався лише нещодавно і новостворені громади потребують організаційної та методичної допомоги для початку реалізації проєктів захисту територій від затоплення [2].

Проаналізувавши останні дослідження та публікації з механізмів функціонування органів державної влади на усіх рівнях, методів та підходів до реалізації та впровадження проєктів захисту населення від затоплення та практики застосування засад управління ризиками виникнення надзвичайних ситуацій (з урахуванням міжнародного досвіду), зроблено висновок, що на сьогоднішній день розроблені моделі управління ризиками виникнення надзвичайних ситуацій лише на державному рівні [2, 3].Як показав аналіз досліджень кращими за ефективністю та тривалістю дії є заходи зроблені на рівні громад. Тому, автори пропонують розробити модель управління ризиками виникнення затоплення територій на рівні ОТГ, в якій детально розписати кожний етап моделі. Крім того, пропонується покроково розібрати процес погодження проєкту, що був обраний в результаті аналізу, з керівництвом громади та мешканцями, а також механізм підготовки проєкту до затвердження з виокремленням можливих джерел фінансування.

Література

1. Офіційний сайт National Intelligence Council – Global Trends. Available at: www.dni.gov/nic/globaltrends.

2. Гаврись , А. ., Яковчук, Р., Стародуб, Ю., & Тур, Н. (2023). Управління ризиками виникнення надзвичайних ситуацій, пов'язаних із затопленням територій на рівні об'єднаних територіальних громад. Науковий вісник: Цивільний захист та пожежна безпека, (1 (15), 101–109. https://doi.org/10.33269/nvcz.2023.1 (15).101-109.

3. Стародуб, Ю. П., Гаврись, А. П., Ковальчук, В. М., Рогуля, А. О., Філіппова, В. Досягнення стабільного розвитку територій шляхом реалізації проєкту визначення зон паводкового затоплення в Україні. Збірник наукових праць Черкаського інституту пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України «Надзвичайні ситуації: попередження та ліквідація». Черкаси. 2022. 6 (1). С.103-114.

УДК 004.6

МОДЕЛЬ КЛАСТЕРИЗАЦІЇ ДАНИХ ДЛЯ ФОРМУВАННЯ ВИБІРКИ З МЕТОЮ ПРОГНОЗУВАННЯ РИЗИКОВИХ СИТУАЦІЙ

Шопський О.М., Придатко О.В.
Львівський державний університет безпеки життєдіяльності

Анотація: в роботі описані основні етапи побудови моделі кластеризації та відбору даних з бази обліку подій системи оперативно-диспетчерського управління. Отримана модель дозволяє здійснювати аналіз, відбір та кластеризацію даних за визначеними подіями із врахуванням фактору людської помилки. Отримана модель орієнтована на формування вибірки з метою подальшого навчання лінгвістичної моделі та прогнозування ймовірності виникнення ризикових ситуацій за визначеними параметрами.

Ключові слова: дані, вибірка, прогнозування, лінгвістична модель.

Abstract: the paper describes the main stages of building a clustering model and data selection from the event accounting database of the operational management system. The resulting model allows for analysis, selection and clustering of data based on certain events, taking into account the factor of human error. The obtained model is focused on the formation of a sample for the purpose of further training of the linguistic model and forecasting the probability of the occurrence of risk situations according to the specified parameters.

Key words: data, sample, prediction, linguistic model.

З метою побудови системи прогнозування ризикових ситуацій та її апробації, потрібно організувати ефективний механізм роботи з даними та формування на їх основі навчальної вибірки. Як було зазначено в попередніх роботах [1, 2] основним джерелом даних для побудови означених моделей, є система оперативно-диспетчерського управління, зокрема її підсистеми щодо зберігання даних про події.

Опис подій, який зберігається у базі даних системи оперативно-диспетчерського управління, містить її коротку характеристику, основні дані про подію, дату її виникнення, час, місце тощо. Наповнення відповідної бази відбувається особовим складом диспетчерської служби в умовах оперативної обстановки. Відтак очевидним є той факт, що в процесі заповнення опису подій можуть виникати помилки пов’язані із людським фактором. З метою пошуку, кластеризації та відбору даних про події за визначеними критеріями, необхідно побудувати ефективну систему, яка дозволятиме уникати технічних та орфографічних помилок на основі семантичних ознак.

Під час побудови означеної моделі, з метою опрацювання даних, використовувалась технологія обробки природної мови – NLP (Natural language processing), зокрема open-source бібліотека Python fastText, яка дозволяє користувачам вивчати і представляти текст для його класифікації. Крім того означена бібліотека дозволяє будувати семантичні зв'язки між словами які використовуються у тексті.

Для вирішення основного завдання, на першому етапі необхідно організувати опрацювання масиву даних для його подальшого аналізу та навчання семантичної моделі. З цією метою за основу взято базу даних системи оперативно-диспетчерського управління Головного управління ДСС України у львівській області від початку її створення (з 2007 року – більше 400 тис. подій).

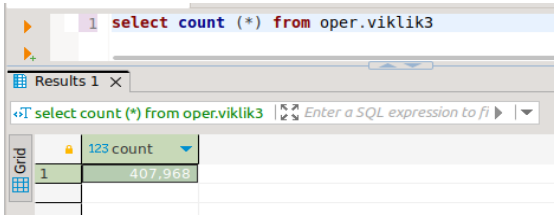


Рисунок 1 – Формування Data-сету з метою формування навчальної вибірки

Для роботи з отриманим Data-сетом запропоновано використання СУБД PostgreSQL. Задля можливості використання повного текстового пошуку у базі даних, до СУБД завантажено великий електронний словник української мови (ВЕСУМ) [3]. Словник можна інтегрувати в різні інформаційні системи. Саме тому для його інтеграції із базою даних проведено компіляцію у відповідний формат (клонування вихідного тексту з github та використання модуля hunspell СУБД PostgreSQL). Нижче наведено приклад використання текстового пошуку, а саме перетворення тексту у вектор слів (без врахування стоп-слів, які не несуть змістового навантаження), із представленням кожного слова у називному відмінку.

```
SELECT * FROM to_tsvector('ukrainian', 'пожеж в приватному господарстві');
'господарство':4 'пожежа':1 'приватний':3
```

Лістинг 1 – Приклад SQL-запиту для формування вектору слів

На другому етапі побудови моделі, необхідно сформувати низку SQL-запитів до бази даних подій. Запити формуються із можливістю ігнорування хибних подій, виїздів підрозділів на навчання, надання платних послуг тощо (до уваги приймаються лише оперативні виїзди).

За результатами аналізу встановлено, що тип події не завжди відповідає його змісту. Цей факт пов’язаний з людським фактором (заповнення даних про подію в оперативній обстановці). Це надає підстави зробити висновок, що задля формування вибірки даних про події, як першоджерело необхідно обирати інформацію не про її тип, а опис самої події, що значно ускладнює процедуру пошуку.

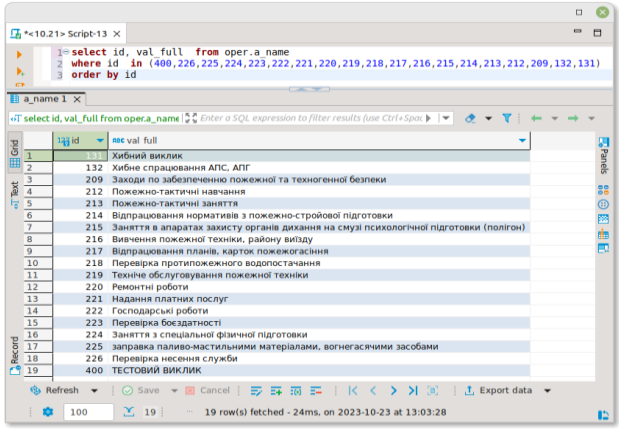


Рисунок 2 – Приклад формування стеку SQL-запитів

Наступним важливим кроком у побудові моделі є очищення даних Data-сету від орфографічних помилок. Для вирішення цього завдання використано бібліотеку Hunspell [4] та обгортку Python – CyHunspell [5]. Для перевірки оффографії та виправлення помилок використано словник ВЕСУМ. Застосування цього інструментарію надало можливість провести аналіз найбільш частих помилок та зберегти їх у довідкову БД.

Висновки. Отже побудова моделі кластеризації даних із системи обліку подій (підсистеми оперативно-диспетчерського управління) надала можливість отримати фекетивний механізм аналізу та відбору даних для формування вибірки з метою прогнозування ризикових ситуацій. Наступним етапом, на основі отриманих вибірок, є навчання лінгвістичної моделі, що є перспективою подальших досліджень.

Література

1. Martyn Ye. Software for Shelter's Fire Safety and Comfort Levels Evaluation / Martyn Ye., Smotr O., Burak N., Prydatko O., Malets I. // Communications in Computer and Information Science, Springer, Cham. – Vol. 1158, 2020. pp. 457-469 https://doi.org/10.1007/978-3-030-61656-4_31

2. 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.

3. Великий електронний словник української мови. [Електронний ресурс]. – Режим доступу: https://github.com/brown-uk/dict_uk

4. Hunspell. About. [Електронний ресурс]. – Режим доступу: https://hunspell.github.io

5. Cyhunspell 2.0.2 [Електронний ресурс]. – Режим доступу: https://pypi.org/project/cyhunspell

УДК 004.4

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ РЕКОМЕНДАЦІЇ КНИГ ІЗ ВИКОРИСТАННЯМ МОДУЛЯ ШІ

Шуригін К. А., Сокольський А. К., Бровко А. А.
Національний університет «Одеська політехніка», Одеса

Анотація. У роботі розглядається інформаційна система, яка дозволяє користувачам отримувати рекомендації книг на основі наданих запитів, попередніх вподобань та звичок.
Ключові слова: рекомендаційна система, машинне навчання.

Abstract. This work considers an information system that allows users to receive book recommendations based on submitted queries, previous preferences and habits.
Keywords: recommendation system, machine learning.

В сучасному світі, більшість інформаційних сфер розваг пропонують механізми рекомендацій, що мають на меті зменшення часу на пошук бажаного результату. Зазвичай, типовими прикладами є сервіси для перегляду серіалів, фільмів, прослуховування музики тощо. Однак, існують певні сфери, де сучасні технології машинного навчання не так широко представлені. Однією з таких є сфера книг. Згідно із дослідженням [1], 75% дорослих в США прочитали книгу в будь-якому форматі за останній рік. Це свідчить про стабільно високий інтерес до читання, що підкреслює необхідність у створення аналогічного до Netflix сервісу для книг.

Ця робота зосереджена на створенні інформаційної системи для надання персоналізованих рекомендацій книг, використовуючи алгоритми машинного навчання та аналізу даних. Система аналізує попередні вподобання користувача, їх читацькі звички, та на основі цього пропонує книги, які максимально відповідають їхнім інтересам. Це схоже на методи, використовувані в алгоритмах рекомендацій, які використовуються на платформах типу Netflix або Spotify, але адаптовані для літературного контенту.

Основна мета роботи полягає у зменшенні часу на пошук книги за особистими вподобаннями. Завдяки інтеграції з різними онлайн-бібліотеками та книгарнями, система здатна пропонувати не тільки цифрові копії книг, але й фізичні екземпляри.

Заходження на шлях рекомендаційних систем часто починається з універсальних рекомендацій [2], де всі користувачі отримують схожі поради щодо книг. Цей підхід, хоч і простий, не враховує індивідуальних вподобань, заснованих на особистих враженнях від попередніх книг, і може обмежувати можливість відкриття нового для читача.

З ростом рівня персоналізації користувач стає активнішим у своєму пошуку, отримуючи рекомендації, які враховують його індивідуальні вподобання. Враховуючи жанри, авторів та конкретні інтереси, система допо-

магає читачеві знаходити книги, які відповідають його унікальному смаку. Це підвищує рівень задоволення від читання і стимулює більше глибоке взаємодії з літературою.

Як показано на рис. 1, рівень персоналізованості рекомендацій лінійно впливає на якість користувальницького досвіду [3].

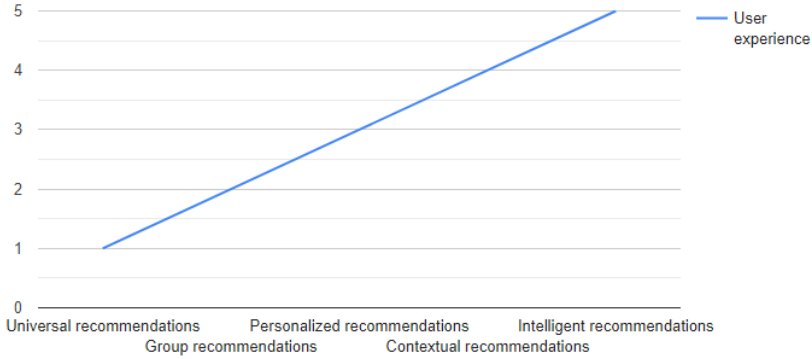


Рисунок 1 – Вплив персоналізованості на якість користувальницького досвіду

Інтерфейс системи розроблено таким чином, щоб бути доступним через різні пристрої, включаючи мобільні додатки та планшети, що забезпечує доступність для широкого кола користувачів. Крім того, система містить спеціальні функції для забезпечення зручності користування людьми з особливими потребами.

В системі передбачено особисті кабінети, де користувачі можуть керувати своїми вподобаннями, переглядати історію читання та отримувати індивідуалізовані рекомендації. Також система включає соціальні функції, де користувачі можуть обговорювати книги, обмінюватися відгуками та рекомендаціями, що сприяє створенню активної читацької спільноти.

На рис. 2 показано усі варіанти використання системи, які визначають функціонал розроблювальної програми. Система декомпозована на 5 модулів та розроблена з дотриманням мікросервісної архітектури (рис. 3). Модуль AuthProxy відповідає за авторизацію та збереження сесій, модуль UserStorage потрібний для збереження та маніпулювання всіма даними користувача, які можуть знадобитись для формування рекомендацій. RecommendationEngine працює зі сховищем книг, він використовує UserStorage та AIModule для безпосереднього формування рекомендацій чи результатів пошуку. ChattingService надає функціонал залишення коментарів, відкриття форумів за темами та персонального чату між користувачами.

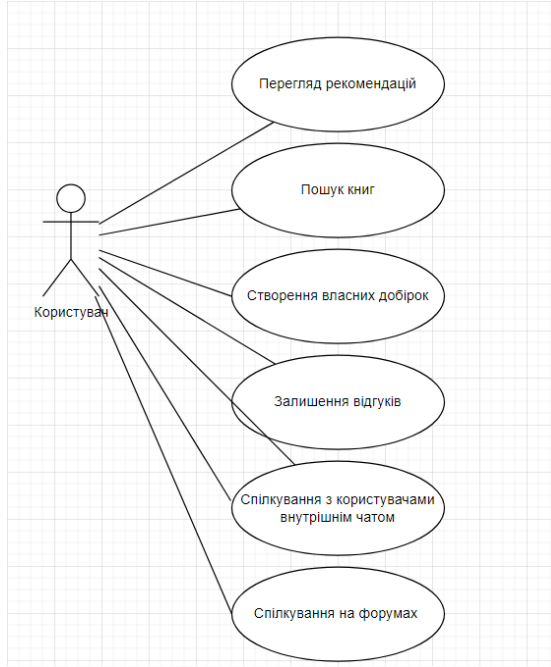


Рисунок 2 – Діаграма прецедентів

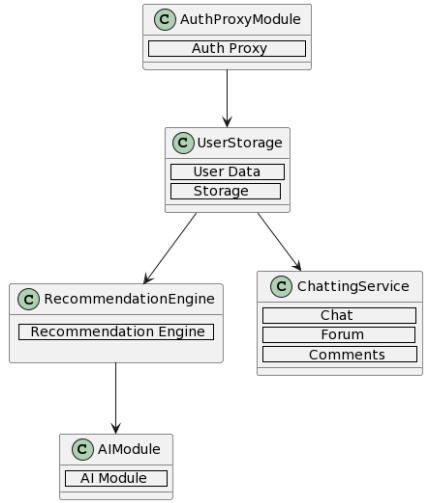


Рисунок 3 – Структура модулів програми

В контексті впливу на освіту та культуру, така система рекомендацій може стати значущим інструментом. Вона не тільки спрощує пошук і вибір літератури, але й може стимулювати інтерес до читання, підвищуючи культурний рівень та освітні можливості суспільства.

Висновки. Виявивши переваги використання рекомендаційних систем в таких сферах, як сфера розваги, торгівлі, туризму було узято їх приклад для створення системи рекомендацій для читачів. У порівнянні із традиційним способом пошуку та вибору книг, розроблена система демонструє:

- Зменшення часу пошуку в 6 разів
- Збільшення рівня персонального задоволення від рекомендації в 3 рази
- Збільшення кількості активних читачів в 2.3 рази

Література

1. Three-in-ten Americans now read e-books. URL: https://www.pewresearch.org/short-reads/2022/01/06/three-in-ten-americans-now-read-e-books/#:~:text=75, unchanged%20since%202011

2. The role of personalized recommendations in customer acquisition. URL: https://aicontentfy.com/en/blog/role-of-personalized-recommendations-in-customer-acquisition#

3. The impact of personalized recommendations on customer experience. URL: https://markettailor.io/blog/impact-of-personalized-recommendations-on-customer-experience

УДК 004.9

ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ У НАВЧАЛЬНИХ ПРОЦЕСАХ

Яковчук В.С., Придатко О.В.
Львівський державний університет безпеки життєдіяльності

Віртуальна реальність (VR) – це технологія, яка створює іммерсивне віртуальне середовище, яке імітує реальний світ або створює абсолютно уявний. Вона використовує комп'ютерну графіку, сенсори та інші пристрої для того, щоб поглибити користувача у віртуальний світ та дозволити йому взаємодіяти з ним.

Використання віртуальної реальності (VR) у навчальних процесах є перспективним інструментом, який змінює парадигму навчання та сприяє поглибленому засвоєнню навчального матеріалу. Ця технологія, завдяки своїй іммерсивності та можливостям візуалізації, відкриває нові можливості для навчання в різних галузях освіти. Для кращого ознайомлення з системою VR технологій, потрібно детальніше зрозуміти її особливості.

Створення іммерсивних навчальних середовищ. Використання VR дозволяє створювати іммерсивні навчальні середовища, які моделюють реальні або уявні сценарії. Це особливо ефективно в галузях, де важливо відчути або взаємодіяти з оточенням, таких як медицина, інженерія або мистецтво.

Поглиблене вивчення складних концепцій. VR дозволяє студентам не лише читати чи дивитися інформацію, але і взаємодіяти з нею. Вивчення абстрактних чи складних концепцій стає більш доступним, оскільки студент може відчути їх у просторі та сприймати за допомогою різних сенсорів.

Симуляція реальних сценаріїв. Використання VR у навчанні дозволяє створювати симуляції реальних сценаріїв, що корисно в тих випадках, коли практичний досвід або взаємодія з реальними об'єктами складна чи небезпечна. Наприклад, медичні студенти можуть тренувати операції у віртуальному середовищі.

Залучення студентів та підвищення мотивації. Віртуальна реальність сприяє залученню студентів до навчального процесу через новаторські технології та цікаві візуальні ефекти. Це може підвищити рівень мотивації студентів, оскільки вони стають активними учасниками навчання.

Можливості індивідуалізації та адаптації. VR дозволяє створювати індивідуальні навчальні траси, адаптовані до потреб кожного студента. Це може сприяти ефективнішому вивченню та враховувати індивідуальні стилі навчання.

Виклики та перспективи. Однак, необхідно враховувати виклики, такі як технічні обмеження, вартість обладнання та можливі проблеми з

здоров'ям. Дослідження і вирішення цих питань є важливим кроком у розвитку використання VR в освіті.

Використання віртуальної реальності стає все більше адаптивним під кожну навчальну програму та галузь освіти не в залежності від особливостей її подання, адже має величезний спектр функцій та різних методів їх використання. Для прикладу опишемо деякі з основних видів освіти та реалізацію їхнього використання VR технологій.

Медична освіта. Віртуальна реальність використовується для тренування студентів на основі візуальної взаємодії з віртуальними об’єктами. Студенти можуть взаємодіяти з тривимірними моделями людського тіла, вивчаючи анатомію та проводячи віртуальні хірургічні операції. Це дозволяє практикувати навички без реального ризику для пацієнта та мати безліч спроб для покращення свого результату.

Хімічна освіта. Використання VR у хімічній освіті дозволяє студентам взаємодіяти з молекулярними структурами та проводити хімічні експерименти у віртуальному середовищі. Це сприяє кращому розумінню хімічних процесів та безпеці під час експериментів, що в свою чергу тягне за собою ще більшу зацікавленість основ вивчення тих чи інших предметів.

Історична освіта. Віртуальна реальність в історичній освіті дозволяє студентам подорожувати у часі, відвідуючи далеку хронологію та місця на яких концентрувалося безліч важливих епіцентрів подій. Це надає можливість отримати живе враження від минулих епох, роблячи навчання більш захопливим.

Мовна освіта (Філологія). У вивченні мов віртуальна реальність може створити іммерсивне оточення, де студенти опиняються у віртуальному середовищі, де вони повинні використовувати ту чи іншу мову для спілкування з віртуальними персонажами або вирішення реальних ситуацій, особливо в поєднанні з штучним інтелектом.

Професійна підготовка. Віртуальна реальність використовується для підготовки фахівців у різних галузях, таких як авіація, будівництво чи виробництво, рятувальних чи екстрених служб. Співробітники можуть тренуватися у віртуальних сценаріях, відтворюючи реальні робочі умови та ситуації в яких ти маєш можливість необмеженої кількості повторювань та відпрацювань.

Астрономічна освіта. Віртуальна реальність дозволяє студентам вивчати астрономію, відвідуючи віддалені планети, спостерігаючи за зорями та вивчаючи космічні об'єкти у віртуальному просторі.

Хоча віртуальна реальність (VR) є потужним інструментом з великим потенціалом застосування, її також супроводжують ряд недоліків та викликів. Ось деякі з найбільш очевидних обмежень та недоліків віртуальної реальності.

Вартість. Обладнання для віртуальної реальності часто є дорогим. VR-окуляри, сенсори та інші компоненти можуть бути високою вартістю, що обмежує доступність технології для більшого кола користувачів.

Фізичні обмеження. Використання VR може викликати фізичні неприємності, такі як головний біль, запаморочення та втома, викликана тривалим користуванням. Деякі люди також можуть відчувати дискомфорт через рухи у віртуальному середовищі, неспівпадання рухів тіла та відчуття в VR.

Відсутність реального взаємодії. У віртуальному світі відсутня реальна фізична тактильна взаємодія з предметами, що може вплинути на реалізм та ефективність навчальних симуляцій чи симуляцій професійних ситуацій.

Технічні обмеження. Технічні обмеження, такі як обмежений обсяг обчислювальних ресурсів та графічні обмеження, можуть вплинути на якість віртуального відображення та загальний рівень іммерсії.

Відсутність стандартів та низька якість контенту. Наразі відсутні стандартизовані правила та норми в галузі віртуальної реальності, що може впливати на сумісність різних платформ та додатків. Хоча технологія виробляється швидко, не завжди забезпечується висока якість контенту. Деякі додатки можуть бути малоіммерсивними або недостатньо цікавими для користувача.

Віртуальна реальність є інноваційною технологією, яка потенційно може трансформувати багато сфер життя, включаючи навчання, медицину, ігри та багато інших. Її використання вже принесло значний внесок у створення іммерсивних навчальних середовищ, симуляцій та без перебільшень корисних додатків. Майбутнє віртуальної реальності залежить від постійних досліджень, розвитку нових технологій та зусиль для вирішення існуючих викликів. Якщо ці проблеми будуть вирішені, віртуальна реальність може стати важливим елементом сучасного суспільства, роблячи істотний внесок у різні галузі освіти.

Література

1. Burdea, G., & Coiffet, P. (2003). Технологія віртуальної реальності. Wiley-IEEE Press.

УДК 159.99

ГЕНДЕР У ПРОФЕСІЙНІЙ САМОРЕАЛІЗАЦІЇ МАЙБУТНІХ РЯТУВАЛЬНИКІВ

Яремко Роман
Львівський державний університет безпеки життєдіяльності

Згідно з обширними соціально-психологічними дослідженнями, самореалізація особистості часто розглядається у контексті професійної самореалізації. Реалізація в професійній сфері описується як процес та результат досягнення людиною максимального рівня особистісного розвитку, можливості використовувати свій потенціал у своїй професії та досягати в ній успіху.
Ключові слова: професійна самореалізація, гендер, рятувальники.

According to extensive social-psychological research, self-realization of an individual is often considered in the context of professional self-realization. Realization in the professional sphere is described as the process and outcome of an individual achieving the maximum level of personal development, the ability to utilize their potential in their profession, and succeed in it.
Key words: professional self-realization, gender, rescuers.

Зрозуміло, що аналіз самореалізації особистості повинен включати в себе дослідження життєвих принципів, цінностей, ідеалів, можливостей та досягнень особистості, а також вивчення різних компонентів самосвідомості на основі психологічної теорії діяльності. Ця теорія дозволяє досліджувати такі аспекти системи діяльності, як мотиви, цілі, важливі професійні якості тощо. Наявність окремих досліджень в рамках цих підходів допомагає сформулювати загальну концепцію самореалізації, що неможливо без розкриття її смислового і процесуального аспектів, а також без визначення структури та особистісних факторів, які впливають на самореалізацію суб'єкта [2]. Професійна самореалізація може бути розглянута у трьох основних контекстах психічних явищ, а саме як процес, стан (на певному етапі) та властивість суб'єкта. Процес самореалізації є найважливішим класом психічних явищ і дозволяє системно досліджувати життєдіяльність людини. Тому самореалізація суб'єкта охоплює свідомий вибір і реалізацію аспектів індивідуальності, які сприяють його самовираженню, використанню потенціалу, створенню власної системи цінностей, мотивів, цілей та методів їх досягнення, включаючи трансформацію самого себе.

Бажання до професійної самореалізації виникає внаслідок незадоволеної потреби у реалізації свого професійного потенціалу, володіння професійними знаннями, вміннями та навичками, а також бажання належати до конкретної професійної спільноти. Також важливою є потреба в профе-

сійній ідентичності, мотивація для досягнення поставлених цілей і отримання задоволення від результатів діяльності. Михайло Ткалич і Людмила Карамушка вважають, що потреба у самореалізації є ключовою складовою формування особистості та сприяє розвитку її професійної зрілості [1].

Професійна діяльність є однією з важливих сфер життя людини, проте розподіл між жінками і чоловіками в економіці, професіях та суспільстві є нерівномірним. Існує ціла низка галузей діяльності та відповідних професій, які традиційно розглядаються як "жіночі" або «чоловічі», і це явище називається «гендерною стратифікацією».

Міф про первинне функціональне призначення жінок і чоловіків впливає на сучасні гендерні відносини, чи навіть можна сказати, їх руйнує. Оскільки гендерні стереотипи щодо професійної самореалізації базуються на переважаючій ролі чоловіків у суспільстві. Проте в історії існують численні приклади, коли жінки активно брали участь у різних видах діяльності, включаючи такі специфічні сфери, як гасіння пожеж та ліквідація наслідків стихійних лих і катастроф.

У працях науковців, таких як Ю. Бохонкова, Н. Вовк, О. Вавринів, Н. Дубчак, О. Кучмєєва, Л. Мандрик, В. Покалюк, Н. Оніщенко, О. Селіванова та інших, детально розглядаються певні аспекти проблеми професійної самореалізації жінок і чоловіків у ризикованих і небезпечних професіях.

У випадку жінок, які несуть службу в пожежно-рятувальних підрозділах, їхню оцінку часто обмежують гендерним підходом, не враховуючи рівень їхньої професійної підготовки. У професійному оточенні рятувальників, жінки можуть стикатися з виключенням через те, що вони не відповідають стандартним практикам їхньої повсякденної діяльності. В той час, як чоловік, незалежно від рівня розвитку професійних якостей, сприймається як колега рятувальника, оскільки чоловік-рятувальник є суспільним стандартом. Незважаючи на цю ситуацію, кількість жінок, які служать в пожежно-рятувальних підрозділах України та інших країн світу, зростає, і це створює нові моделі гендерних особливостей в рятувальних підрозділах.

Аналіз наукової літератури показує, що фемінізація пожежно-рятувальних служб в різних країнах світу продовжується і має загальні тенденції розвитку, але також має свої специфічні особливості, які залежать від традицій та культури відповідних регіонів. Зміни в законодавстві сприяли підвищенню ролі пожежних служб та дозволили жінкам здійснювати більше функцій у галузі пожежної безпеки. Раніше жінки обмежувалися пожежною профілактикою та наданням домедичної допомоги, але зараз зростає кількість жінок, які беруть участь у гасінні пожеж.

Часто жінкам відмовляють у можливості служби в аварійно-рятувальних підрозділах, пояснюючи це тим, що вони вважаються недостатньо фізично та психологічно підготовленими, порівняно з чоловіками, які, на думку багатьох, мають більше відповідних якостей. Проте досвід

діяльності рятувальників свідчить про те, що успішне виконання професійних обов'язків в службі ДСНС потребує не лише глибоких професійних знань, навичок і вмінь, але й наявність специфічних психологічних якостей. Професійна діяльність рятувальників пов'язана з великим емоційним навантаженням і ризиком для життя, тому бажання допомогти і врятувати життя людей часто переважає над страхом перед можливою небезпекою і смертельними ризиками.

Часто жінкам відмовляють у можливості приймати участь у службі в аварійно-рятувальних підрозділах, обґрунтовуючи це тим, що вони, на їхню думку, не мають необхідних фізичних та психологічних якостей, які, як вважається, зазвичай притаманні чоловікам. Проте практика рятування постраждалих свідчить, що для успішного виконання професійних обов'язків працівників служби ДСНС потрібні не лише глибокі та різноманітні професійні знання, навички та вміння, але також спеціальні психологічні якості. Робота рятувальників пов'язана з великим психоемоційним навантаженням та ризиком для життя, і тут саме бажання допомогти людям, у багатьох випадках, переважає над страхом перед смертю, що дозволяє виконувати професійні завдання.

Готовність працювати в умовах надзвичайних ситуацій і екстремальних обставин в значній мірі визначається наявністю стійкої внутрішньої мотивації для надання необхідної допомоги постраждалим людям, які її потребують. Звісно, наявність лише психологічних якостей не гарантує повного успіху у професії рятувальника, і для цього також потрібно розвивати такі якості, як фізична витривалість, стійкість до фізичних впливів та інші, які переважно характерні для чоловіків.

Література

1. Карамушка Л. М., Ткалич М. Г. Самоактуалізація менеджерів у професійно- управлінській діяльності (на матеріалі діяльності комерційних організацій) : монографія. Запоріжжя : «Просвіта», 2009. 262с.

2. Yaremko, R., Vavryniv, O., Tsiupryk, A., Perelygina, L., & Koval, I. Research of content parameters of the professional self-realization of future fire safety specialists. Amazonia Investiga. 2022. № 11(53). P. 288-297. https://doi.org/10.34069/AI/2022.53.05.28

З М І С Т

Секція 1

КІБЕРБЕЗПЕКА

Секція 2

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VI Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

Відповідальні за випуск **Олександр Придатко**
Назарій Бурак

Оригінал-макет **Олександр Хлевной**

Підписано до друку 22.12.2023 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 30.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.
e- mail: mail@ubgd.lviv.ua, kafedra.itts@gmail.com