



softserve



ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

**Збірник наукових праць
V Міжнародної науково-практичної
конференції
ІБІТ 2024**

27 листопада 2024 року

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

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІБІТ 2024

Збірник наукових праць
V Міжнародної науково-практичної конференції

27 листопада 2024 року

Львів – 2024

ББК 32.81+78.362

I 74

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

ISBN 978-617-8537-86-9

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.

© ЛДУ БЖД, 2024

ISBN 978-617-8537-86-9

© Видавництво «Растр-7», 2024

ЧЛЕНИ ПРОГРАМНОГО КОМІТЕТУ:

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

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

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

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

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

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

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

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

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

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

сор кафедри захисту інформації Національного університету “Львівська політехніка”.

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

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

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

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

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

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

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

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

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

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

РЕДКОЛЕГІЯ:

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

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

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

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

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

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

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

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

Любомир СІКОРА – д.т.н., професор, професор кафедри автоматизованих систем управління Національного університету “Львівська політехніка”.

Наталія ЛИСА – д.т.н., доцент, доцент кафедри автоматизованих систем управління Національного університету “Львівська політехніка”.

Тетяна ГОВОРУЩЕНКО – д.т.н., професор, декан факультету інформаційних технологій Хмельницького національного університету.

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

Ольга МЕНЬШИКОВА – к.ф.-м.н., доцент, заступник начальника факультету цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи.

Андрій ІВАНУСА – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності.

Валентина ЯЩУК – к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності.

Орест ПОЛОТАЙ – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності.

Валерія БАЛАЦЬКА – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності.

Ігор МАЛЕЦЬ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

Назарій БУРАК – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

Ольга СМОТР – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

Юрій БОРЗОВ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

Роман ГОЛОВАТИЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

Олександр ХЛЕВНОЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

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.

Інформаційні джерела

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. The MIT Press, 2016, 800 p.
2. Shorten C., Khoshgoftaar T. M. A survey on Image Data Augmentation for Deep Learning. Journal of Big Data, 2019, Vol. 6, No. 1, pp. 1–48.
3. Tan M., Le Q. V. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. International Conference on Machine Learning (ICML), 2019, pp. 6105–6114.
4. Krizhevsky A., Sutskever I., Hinton G. E. ImageNet Classification with Deep Convolutional Neural Networks. Advances in Neural Information Processing Systems (NeurIPS), 2012, pp. 1097–1105.
5. He K., Zhang X., Ren S., Sun J. Deep Residual Learning for Image Recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 770–778.
6. Powers D.M.W. Evaluation: from Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation. Journal of Machine Learning Technologies, 2011, Vol. 2, No. 1, pp. 37–63.

УДК 004.432.4

МОДЕЛЬНО-ОРІЄНТОВАНИЙ ПІДХІД ДО АВТОМАТИЗАЦІЇ ГЕНЕРАЦІЇ ТЕСТОВИХ ВИПАДКІВ НА ОСНОВІ UML ДІАГРАМ

*Марта ЛІННИК
Юлія НАЗАР*

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

Abstract. *This paper describes an approach to automating the process of generating test cases based on UML models. Various UML diagrams are considered for test generation, including Use Case Diagram, Class Diagram, Sequence Diagram, Use Case templates, and a data dictionary expressed in OCL. The methodology ensures automation of the testing process without significant modifications to the initial models.*

Keywords: *UML models, class diagram, position diagram, test-cases, test process.*

Анотація. *В даній роботі описано підхід до автоматизації процесу генерації тест-кейсів на основі UML моделей. Для генерації тестів розглядаються різні UML діаграми, зокрема діаграма варіантів використання, діаграма класів, діаграма послідовностей, шаблони варіантів використання та словник даних, виражений в OCL. Методологія забезпечує автоматизацію процесу тестування без складних змін у початкових моделях.*

Ключові слова: *UML діаграми, діаграма класів, діаграма послідовностей, тест-кейси, процес тестування.*

Відомо, що традиційне тестування зазвичай створює тестові сценарії, ґрунтуючись на вихідному коді програми. Для цього програму перетворюють у різні високорівневі моделі, такі як діаграми керування потоком,

графи потоків даних або графи викликів. Загалом це називається тестуванням на основі моделей. Простими словами – це техніка тестування програмного забезпечення, за якої поведінка тестованого програмного забезпечення під час виконання перевіряється на прогнози, зроблені моделлю, де модель – це опис поведінки системи. У такому підході тести створюються на основі абстрактних моделей програмного забезпечення, зокрема формальних специфікацій або UML-діаграм, які є напівформальними описами дизайну. Автоматична генерація тестових випадків із напрямку з UI моделей має значні переваги. Процес створення тестів вручну є трудомістким і вимагає багато часу та ресурсів, тому автоматизація цього процесу дозволяє суттєво зменшити затрати, забезпечуючи швидке та ефективне тестування. Ще однією перевагою є те, що тест-кейси можна створювати на ранніх етапах розробки, ще до написання програмного коду. Це дає змогу розробникам використовувати готові тести під час створення коду, що зменшує кількість повторних перевірок і циклів між розробкою та тестуванням, додатково економлячи ресурси.

Unified Modeling Language (UML) стала універсальною мовою для моделювання програмних систем. Вона використовується для специфікації, візуалізації, побудови та документування різноманітних компонентів програмного забезпечення. Особливо корисними для тестування є діаграми послідовностей, які фіксують взаємодію між об'єктами у часі. Ці діаграми детально описують взаємодію між компонентами системи, що робить їх природним джерелом для інтеграційного тестування. Системне тестування часто вважається найскладнішим і найретельнішим видом тестування, оскільки воно охоплює всі аспекти функціонування системи.

Для створення тест-кейсів потрібно трансформувати діаграми варіантів використання (UD), діаграми класів (CD) та діаграми послідовностей (SD) у спеціальне представлення, яке називається графом діаграми послідовностей (SDG). Кожен вузол цього графа містить необхідну інформацію для генерації тест-кейсів. Ця інформація збирається з різних джерел: шаблону варіанта використання (також відомого як розширений варіант використання), діаграм класів і словника даних, представленого у вигляді обмежувальних виразів мовою OCL (Object Constraint Language). Наступним кроком є обхід графа SDG для створення тестових випадків відповідно до заданих критеріїв покриття та обраної моделі помилок. Схематична блок-діаграма такого підходу зображена на рисунку 1.

Для розуміння системи в цілому відбувається створення діаграми випадків використання, діаграми класів та діаграми послідовностей. UML-діаграми будуємо за допомогою інструменту Draw.io, оскільки цей інструмент має хорошу підтримку для виразів OCL та є більш зручним порівняно з іншими інструментами. Рисунок 2 представляє діаграму послідовностей для сайту для моніторингу повітряних тривог, зокрема для сценарію перегляду актуальних тривог та попереджень.

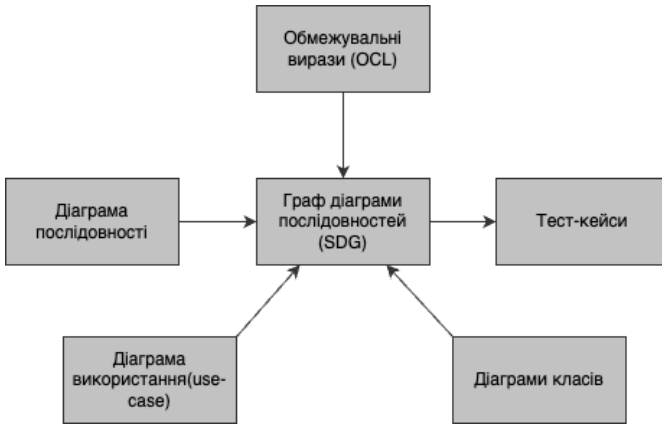


Рисунок 1 – Діаграма для запропонованого підходу

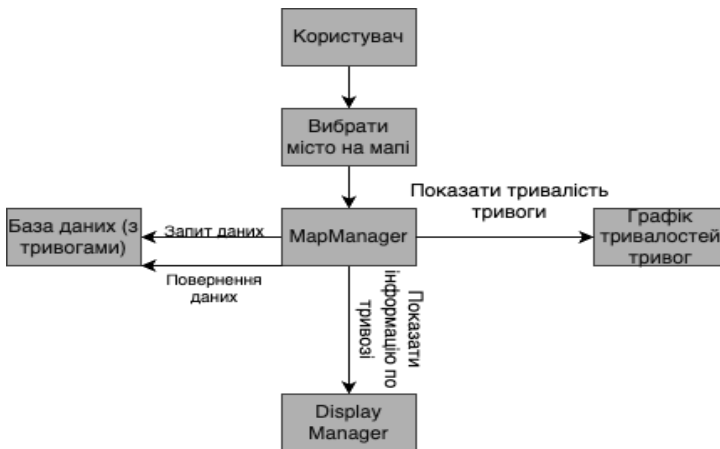


Рисунок 2 – Діаграма послідовностей для Мапи тривог

Парсер працює так, що він читає XML файл, експортований на попередньому етапі, та надає опис усіх тегів і атрибутів з цього файлу. Ця інформація є важливою для генерації опису діаграми послідовностей у вигляді графа, який містить вузли, що зберігають необхідну інформацію для створення сценаріїв. У проєкті використовується API на основі дерева, до прикладу Document Object Model (DOM), яке буде деревоподібну репрезентацію XML-документа в пам'яті. Це API надає класи та методи, які дозволяють програмі здійснювати навігацію та обробляти дерево, що є основою для подальшої обробки даних з XML файлу. Такий підхід дозволяє ефективно пра-

цювати з великими обсягами структурованої інформації та зберігати її у вигляді, зручному для подальшої генерації тестів або створення графів на основі UML-діаграм.

```

<stateX>
S1: null citySelected :MapManager :CitySelector uml:Message
S2: null requestAlertData :MapManager :AlertDatabase uml:Message
S3: null receiveAlertData :AlertDatabase :MapManager uml:Message
S4: null displayAlertInfo :MapManager :DisplayManager uml:Message
S5: null showAlertDuration :MapManager :DurationGraph uml:Message
context MapManager::displayAlertInfo(); pre: AlertDatabase.alerts="CityAlerts"; post: result="Display
city alert data including duration & chart" OCL2.0 uml:OpaqueExpression
<StateY>

<StateX>
S1: null mapOpened :MapManager :DisplayManager uml:Message
S2: null selectAlertType :MapManager :AlertSettingsManager uml:Message
S3: null displayAlertTypes :AlertSettingsManager :DisplayManager uml:Message
S4: null alertTypeSelected :AlertSettingsManager :MapManager uml:Message
S5: null updateAlertMap :MapManager :MapEditor uml:Message
context MapManager::updateAlertMap(); pre: AlertSettingsManager.alertType="SelectedType"; post:
result="Map updated with selected alert type" OCL2.0 uml:OpaqueExpression
S6: null alertTypeChanged :MapManager :AlertSettingsManager uml:Message
S7: null refreshMapDisplay :MapManager :DisplayManager uml:Message
<StateY>
    
```

Рисунок 3 – Вивід згенерованих сценаріїв

Графічне відображення вузлів, що йдуть від StateX до StateY зображене на рисунку 4. Спочатку відображаються всі вузли першого сценарію, після чого, можна по черзі обирати та бачити вузли решти сценаріїв. Цей підхід дозволяє користувачу наочно переглядати різні етапи виконання сценаріїв та зв'язок між різними вузлами, що представляють послідовність подій і дії системи.

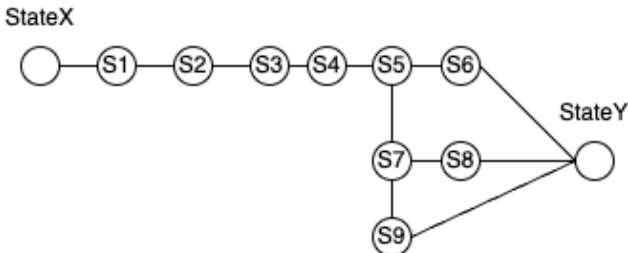


Рисунок 4 – Відображення графа діаграми послідовностей

Висновки. У результаті виконання даного дослідження розроблено модельно-орієнтований підхід для автоматизації генерації тестових випадків програмної системи із використанням UML діаграм. Представлено методологію перетворення UML діаграми послідовностей у граф послідовностей (SDG),

який слугує основою для подальшої автоматизації тестування. Запропонований підхід включає етапи аналізу та парсингу XML-файлів UML діаграм, побудову графа сценаріїв і використання цього графа для створення тестових випадків. Методологія забезпечує автоматичне виділення інформації про передумови, післяумови та повідомлення між об'єктами на основі OCL-виразів, що дозволяє генерувати тестові сценарії без необхідності внесення змін до початкових UML-моделей. Це значно скорочує час на розробку тестів, мінімізує людські помилки та сприяє підвищенню якості програмного забезпечення. Автоматизація на основі запропонованої методики дозволяє ефективніше реалізовувати процеси валідації та перевірки програмних систем, орієнтованих на безпеку або інші критично важливі області застосування.

Інформаційні джерела

1. Смотр О. О., Придатко О. В., Малець І. О. Основи програмування (Python, Java). Львів, 2019. – С. 28 – 74.
2. Коберник С. О., Тарасенко В. О. Моделювання процесів проектування програмного забезпечення на основі діаграм послідовностей UML. Вісник Національного університету “Львівська політехніка”, серія “Інформатика, обчислювальна техніка та автоматизація”, 2020, №15. – С. 82–90.
3. Хом’як В. О., Андрущенко О. В. Автоматизоване тестування програмних продуктів на основі поведінкових моделей. Інформаційні системи і технології в медицині, том 3, № 2, 2022. – С. 39, 47.
4. Мельник І. М., Копайгора О. В. Моделювання та автоматизоване тестування програмного забезпечення на основі графів. Вісник НТУ “ХПІ”. Серія: Інформатика та моделювання, випуск 1, 2021. – С. 57–62.

УДК 004.942:681.625.23

МОДЕЛЮВАННЯ ТА АНАЛІЗ ПРОЦЕСУ ОФСЕТНОГО ДРУКУ

Михайло ВЕРХОЛА

Національний університет “Львівська політехніка”, м. Львів, Україна.

***Abstract.** This paper proposes a computer technology for analyzing the ink transfer process in offset printing systems, which makes it possible to obtain information about the required parameters of the ink and wetting solution input before printing, which significantly reduces the time required to prepare offset machines for printing.*

***Keywords:** inkjet printing system, offset printing, computer modulation, wetting solution, emulsified ink, simulator.*

***Анотація.** В даній роботі пропонується комп'ютерна технологія аналізу процесу передачі фарби у фарбодрукарських системах офсетного типу, яка дає можливість отримувати інформацію про необхідні параметри вхідного завдання фарби і*

Інформаційні джерела

1. FlameSim. URL: <https://www.flamesim.com>
2. FireRescue1 Academy. URL: <https://www.firerescue1academy.com>
3. Pixaera. Revolutionize Safety Training with Pixaera's Immersive Learning Platform. URL: https://pixaera.com/revolutionalize-your-ehs-training/?utm_source=google&utm_medium=CPC&utm_campaign=tofu&utm_term=safety%20management%20training&utm_term=safety%20management%20training&utm_campaign=ToFu+Europe&utm_source=adwords&utm_medium=ppc&hsa_acc=9521312752&hsa_cam=21828056107&hsa_grp=167732076143&hsa_ad=717672807354&hsa_src=g&hsa_tgt=kwd-80708811&hsa_kw=safety%20management%20training&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gad_source=1&gbraid=0AAAAA-MvwtW8WT9rNJvODvq3ENg0OwZ1s&gclid=Cj0KCQiAgJa6BhCOARIsAMiL7V_yW-JIRkkEQky5U85hS28XxlUkAdDJCN0asRGnbaioKF8OL_opIXEaAk0DEALw_wcB
4. Flaim. FLAIM Trainer™, the world's first immersive technology enabled firefighter training solution. URL: <https://flaimsystems.com/products/trainer>

З М І С Т

СЕКЦІЯ 1

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

НАПРЯМ 1.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ВІЙНИ

Балацька В., Побережник В. ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ТА NFT ДЛЯ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ДЕРЖАВНИХ РЕЄСТРІВ	6
Фединець Н., Синиця О. МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В СУЧАСНИХ РЕАЛІЯХ	9
Полотай О. ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ПОТОКІВ БАНКІВСЬКОЇ УСТАНОВИ	12
Ткаченко А. ВІРУСИ-ДРОППЕРИ: ТЕХНІКИ ДОСТАВКИ ШКІДЛИВОГО ПЗ ТА ОБХІД ЗАХИСНИХ СИСТЕМ	16
Яшук В., Ошурко Б. СУЧАСНІ ВИКЛИКИ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ В УМОВАХ ВІЙНИ	17
Яшук В., Столярчук В. ОЦІНЮВАННЯ ВПЛИВУ ШТУЧНОГО ІНТЕЛЕКТУ НА СИСТЕМУ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ ..	20
Виглазов В. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ВОЄННИЙ ЧАС	23
Паньків А-М-І., Хлевной О. КІБЕРЗАГРОЗИ ПІД ЧАС ВІЙНИ: ТАКТИКИ, МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ	27
Бик Е., Бурак Н. ДОСЛІДЖЕННЯ СУЧАСНИХ КОМУНІКАЦІЙНИХ ПЛАТФОРМ ДЛЯ ОПТИМІЗАЦІЇ ТА АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ПОВСЯКДЕННОЇ ДІЯЛЬНОСТІ ДСНС УКРАЇНИ	29
Водоніс Я., Полотай О. ПРОЦЕСНИЙ ПІДХІД В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВАХ, ЯКІ НАДАЮТЬ ІТ-ПОСЛУГИ	32
Литвиненко Р., Лучик В. ЦИФРОВА КРИМІНАЛІСТИКА	36
Мукан І., Котовська О. КРИМІНАЛЬНО-ПРАВОВІ ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У КІБЕРПРОСТОРИ ТА ЕКСПЕРТНА РОЛЬ ГРОМАДСЬКИХ (НЕУРЯДОВИХ) ОРГАНІЗАЦІЙ	39

Ящук В., Водницька О., Sharadze A. АНАЛІЗ СВІТОВИХ ПРАКТИК УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ПРИ ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ	43
Дем'яничук Ю. МОДЕЛЬ ПОВЕДІНКИ “АГЕНТІВ” ВОЄННОЇ КОМУНІКАЦІЇ: ФОРМАЛЬНО-СИНТАКСИЧНА ІЄРАРХІЯ	47
Харчук А.І., Харчук А.А. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВІЙНИ	51
Бундус В., Лучик В. РОЗСЛІДУВАННЯ КІБЕРАТАК У ВОЄННИХ УМОВАХ	53

НАПРЯМ 2.

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В ПІДРОЗДІЛАХ МВС УКРАЇНИ

Борматов Р. ПРОТИДІЯ ВИТОКУ ІНФОРМАЦІЇ З ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ В ПІДРОЗДІЛАХ МВС УКРАЇНИ .	56
Пилипенко В., Тимчишин О., Федець Н. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В ОРГАНАХ ТА ПІДРОЗДІЛАХ ДСНС УКРАЇНИ	59

НАПРЯМ 3.

БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Savchuk K. AI IN ACTION: DEFENDING AGAINST EVOLVING CYBER THREATS	63
Орощук Х., Маслова Н., Любименко О. ЗАГРОЗИ CLOUD COMPUTING: ВИКЛИКИ ТА МЕТОДИ ЗАХИСТУ	67
Івануса А., Ткаченко А., Петрович А. ВДОСКОНАЛЕННЯ АРХІТЕКТУРИ ЗАСОБІВ АВТОМАТИЗОВАНОГО ПОШУКУ ВРАЗЛИВОСТЕЙ WEB-ДОДАТКІВ	72
Кондратюк М. ЗАХИСТ КРИПТОВАЛЮТНИХ ГАМАНЦІВ	75
Івануса А., Брич Т., Ткач М. РОЗРОБКА МОДУЛІВ І ФУНКЦІОНАЛЬНОСТІ ЗАСОБУ АВТОМАТИЗОВАНОГО ПОШУКУ ВРАЗЛИВОСТЕЙ	78
Грабченков Б., Лучик В. СИСТЕМА ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ТА ЇХ ЗАСТОСУВАННЯ	82
Івануса А., Сорока А., Ланчевич А. АНАЛІЗ МЕТОДІВ ТА ІНСТРУМЕНТІВ ДЛЯ ПОШУКУ ВРАЗЛИВОСТЕЙ У WEB-ДОДАТКАХ	85

НАПРЯМ 4.

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Раповук У., Раповук R., Rajesh N., Fedyna B. SECURE DOCUMENT MANAGEMENT VIA VPN IN CORPORATE INFORMATION SYSTEMS	89
Сабадах І., Лучик В. РОЛЬ ШИФРУВАННЯ У ЗАБЕЗПЕЧЕННІ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ	93
Гордієнко Т. АНАЛІЗ ЗАГРОЗ У КАНАЛАХ ЗВ'ЯЗКУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ОПЕРАТИВНОЇ ПОЛІГРАФІЇ	96
Світличний В., Шестаков В. МЕТОДИ ЗАХИСТУ ІОТ-ПРИСТРОЇВ ВІД КІБЕРЗАГРОЗ	100
Клименко Т. АКТУАЛЬНІСТЬ ЗАХИСТУ Й БЕЗПЕКИ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ І МЕСЕНДЖЕРАХ В УМОВАХ ВІЙСЬКОВОГО СТАНУ	105
Ящук В., Кутник Н. ОЦІНЮВАННЯ ВРАЗЛИВОСТЕЙ У ВІРТУАЛЬНИХ СЕРЕДОВИЩАХ З ВИКОРИСТАННЯМ ПЛАТФОРМИ TRUНАСКМЕ	107
Любимов О., Іовенко І. МОДЕЛЬ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ЗВ'ЯЗКУ З ОРБІТАЛЬНИМИ НАНОСУПУТНИКАМИ	110
Остапець Д., Сухомлин О. ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДИК ФОРМУВАННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ	116
Остапець Д., Мотиленко В. МОЖЛИВОСТІ ВИКОРИСТАННЯ ДОКАЗІВ НУЛЬОВОГО РОЗГОЛОШЕННЯ У СИСТЕМАХ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ	119
Курінний І., Світличний В. АНТИВІРУСНІ ПРОГРАМИ: ЇХ ЗНАЧЕННЯ ТА ЕФЕКТИВНІСТЬ У ЗАХИСТІ ДАНИХ	122
Лучик В., Прокопчук Н. ЗАХИСТ СИСТЕМ УПРАВЛІННЯ ПРОМИСЛОВИМИ ПРОЦЕСАМИ (SCADA)	124
Полотай О. ДОСЛІДЖЕННЯ СПОСОБІВ ЗАХИСТУ WEB-САЙТІВ ВІД МЕРЕЖЕВИХ АТАК	128
Одерій Н., Світличний В. ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРЗЛОЧИННОСТІ: МОТИВАЦІЯ ЗЛОВМИСНИКІВ	131
Федоренко А. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВУ ЕПОХУ: НОРМАТИВНО-ПРАВОВИЙ АСПЕКТ	134
Полотай О., Гуменюк М. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ БЕЗПЕЧНИХ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ VLAN	136

Пільов К. ШТУЧНИЙ ІНТЕЛЕКТ В ПРОТИДІ КІБЕРЗЛОЧИННОСТІ	140
Литвиненко Р., Лучик В. ОСНОВНІ ПРОТОКОЛИ МЕРЕЖЕВОЇ БЕЗПЕКИ	143
Рошинець І., Полотай О. ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ VPN	146
Лучик В., Гуменюк І. БРАНДМАУЕРИ ТА ЇХ ВИКОРИСТАННЯ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ	150
Світличний В., Колода Я. БЕЗПЕКА ЕЛЕКТРОННОЇ ПОШТИ: МЕТОДИ ЗАХИСТУ ВІД СПАМУ ТА ШКІДЛИВИХ ВКЛАДЕНЬ ...	154
Ориник С., Полотай О. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ЗАХИСТУ ВІД АТАК VLAN HOPPING	157
Курило Д., Світличний В. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОТИДІ ІНТЕРНЕТ ПІРАТСТВУ	159
Назаров В. ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ МІЖНАРОДНОЇ РЕКЛАМНОЇ АГЕНЦІЇ В УМОВАХ ДЕЦЕНТРАЛІЗОВАНОГО СЕРЕДОВИЩА	161
Філіпчук Б., Ткачук Р. ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАХИЩЕНИХ КАНАЛІВ, ПОБУДОВАНИХ НА ПРОТОКОЛАХ WireGuard ТА OpenVPN	166
Світличний В., Ковтун І. СУЧАСНІ МЕТОДИ БОРОТЬБИ З АТАКАМИ ТИПУ SQL-ІН'ЄКЦІЙ	171
Кугот В., Сабат В. ОПЕРАТИВНЕ УПРАВЛІННЯ В ІЄРАРХІЧНО-СТРУКТУРОВАНИХ СИСТЕМАХ ТА ВИБІР МОДЕЛЕЙ СТРАТЕГІЙ ЦІЛЕОРІЄНТОВАНИХ ДІЙ В УМОВАХ ЗАГРОЗ	173
Гончарук І., Манжай О. ЗАХИСТ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ: ПРАКТИКИ ТА ПЕРСПЕКТИВИ В УКРАЇНІ	177
Руденко М. ОКРЕМІ АСПЕКТИ ПРОТИДІ КІБЕРШАХРАЙСТВУ ...	179
Нечипорук В., Лучик В. АНАЛІЗ ВРАЗЛИВОСТЕЙ В ПОПУЛЯРНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ ТА ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ	181
Дмитрук Б., Степанчук Н., Бурак Р. ЗАХИСТ ВІД ФІШИНГУ ТА РИЗИКИ ВІДКРИТИХ ДЖЕРЕЛ	185

НАПРЯМ 5.

ГЕНДЕР У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Яхно Н., Лучик В. ГЕНДЕР У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ..	189
Шевців Ю., Костишин Е. ВПЛИВ ВІЙНИ НА ГЕНДЕРНУ ПАРИТЕТНІСТЬ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ	192

Яремко Р., Ткачик О. ПОНЯТТЯ ПРО ГЕНДЕРНІ СТЕРЕОТИПИ ТА ЇХ ВПЛИВ НА ПОВСЯКДЕННЕ ЖИТТЯ ЛЮДЕЙ	194
Коваль І., Лакіш В. ГЕНДЕРНІ ВІДМІННОСТІ У ПІДГОТОВЦІ РЯТУВАЛЬНИКІВ	196

НАПРЯМ 6.

КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Grytsiuk P., Sikora L. THE MECHANISM OF GENERATING FIBONACCI AND LUCAS POLYNOMIALS	199
Weigang G., Myronchuk K. DATA ENCRYPTION ALGORITHMS IN MASS SERVICE SYSTEMS	204
Чорненко С., Манжай О. КРИПТОГРАФІЧНІ МЕТОДИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ	208
Demydova A., Maslova N., Kis T. ЗАСТОСУВАННЯ МЕТОДІВ ШИФРУВАННЯ В СИСТЕМАХ ЗАХИСТУ МЕДИЧНИХ ДАНИХ ...	212
Кобилкіна О., Ровецький І. СУЧАСНІ КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ	216
Остапець Д., Дзюба В. АПАРАТНИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ	219
Галицький І., Лаврик Т. ІНТЕГРАЦІЯ КРИПТОГРАФІЇ ТА СТЕГАНОГРАФІЇ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ: АНАЛІЗ ПРОГРАМНИХ РІШЕНЬ	222
Горячий О., Журавель І. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПРОСТИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ОБРОБКИ ЦИФРОВИХ ЗОБРАЖЕНЬ ІЗ ВИКОРИСТАННЯМ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ	226
Малець О.-С., Смотр О. СТАН ДОСЛІДЖЕНЬ У СФЕРІ ЦИФРОВОГО МАРКУВАННЯ ДЛЯ АУДІОФАЙЛІВ	231
Горячий О., Яремчук З. АНАЛІЗ ЕФЕКТИВНОСТІ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ КВАДРАТНОГО КОРЕНЯ ПРОСТОГО ЧИСЛА	234

НАПРЯМ 7.

КІБЕРБЕЗПЕКА ІНФРАСТРУКТУРИ

Ranovuk U., Hidey R. HARDWARE-SOFTWARE APPROACH TO ENSURING INFORMATION SECURITY IN AUTOMATED METROLOGICAL CONTROL SYSTEMS FOR PRODUCTION PROCESSES	238
--	-----

Ranovyk U., Kutas S., Qureshi A. SECURE ACCESS TO ENTERPRISE INFORMATION SYSTEMS IN THE MODERN DIGITAL ENVIRONMENT	242
Чепурной К., Тимошенко Л. ЗАХИСТ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ	247
Танчин І. СТРАТЕГІЇ РЕАЛІЗАЦІЇ ЗАХОДІВ КІБЕРБЕЗПЕКИ В АРХІТЕКТУРІ ІоТ ПОЛІГРАФІЧНОГО ПІДПРИЄМСТВА	250
Балацька В., Опірський І. ТЕХНОЛОГІЯ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ ДОВІРИ ТА ПРОЗОРОСТІ У ДЕРЖАВНИХ РЕЄСТРАХ	254
Лиса Н., Ткачук Р., Сидоренко О. ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ КОГНІТИВНОЮ СИСТЕМОЮ ОСОБИ В УМОВАХ ДІЇ АКТИВНИХ ЗАГРОЗ	256
Сікора Л., Лиса Н., Ткачук Р., Федевич О. ІНТЕЛЕКТУАЛЬНІ ТА ПСИХОЛОГІЧНІ ХАРАКТЕРИСТИКИ ОСОБИ ЯК УПРАВЛІНСЬКОГО ЕЛЕМЕНТУ ІНТЕГРОВАНИХ СИСТЕМ	261
Сікора Л., Якимчук Н. ІНТЕГРАЦІЯ ТЕХНОГЕННИХ ІЄРАРХІЧНИХ СИСТЕМ УПРАВЛІННЯ ПРИ ДІЇ ФАКТОРІВ ЗАГРОЗ	269
Федина Б., Лисий Ю., Сидоренко Р. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ СТВОРЕННЯ СЦЕНАРІЇВ ДІАЛОГУ ДЛЯ УПРАВЛІННЯ В ІЄРАРХІЇ АСУ-ТП ІНФРАСТРУКТУРИ	276
Піх І., Браташ С. ВІДМОВСТІЙКІСТЬ ЯК КРИТЕРІЙ ЯКОСТІ ВЕБЗАСТОСУНКУ	284
Побережник В., Балацька В., Опірський І. КОНЦЕПЦІЯ САМОСУВЕРЕННОЇ ІДЕНТИЧНОСТІ ЯК АЛЬТЕРНАТИВА ТРАДИЦІЙНИМ МЕТОДАМ АВТЕНТИФІКАЦІЇ	288
Ротань К. КРИТИЧНА ІНФРАСТРУКТУРА ПІД ЧАС ВІЙНИ: ЗАХИСТ ВІД КІБЕРАТАК ТА ВІДНОВЛЕННЯ СИСТЕМ	291
Коробейнікова Т., Одінцов Б. ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБМІНУ ПОВІДОМЛЕННЯМИ	294
Дейнека О., Гарасимчук О. МОДЕЛЬ КЛАСИФІКАЦІЇ ІНФОРМАЦІЇ ЗГІДНО З ВИМОГАМИ SOC 2 TYPE 2	298
Сафронов О., Лучик В. ВПЛИВ СУЧАСНИХ ЗАГРОЗ НА КІБЕРБЕЗПЕКУ ТА ЕФЕКТИВНІСТЬ ПІДХОДІВ ДО ЇХ ЗАПОБІГАННЯ ..	302
Рак М. ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРЗЛОЧИНИ: КРИМІНАЛЬНА ТА ЦИВІЛЬНА. СОЦІАЛЬНО-ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ	304
Дурняк Б., Ткачук Р., Сікора Л. ІДЕНТИФІКАЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ДІЯЛЬНОСТІ КОГНІТИВНОЇ СИСТЕМИ ОСОБИ В УМОВАХ ДІЇ АКТИВНИХ ЗАГРОЗ	307

Хиляк Н., Лиса Н., Тупичак Л., Бохан О., Бохан М. МОДЕЛІ КООРДИНАЦІЙНИХ СТРАТЕГІЙ ПРИЙНЯТТЯ РІШЕНЬ В ІЄРАРХІЧНИХ КІБЕР ТЕХНОГЕННИХ СИСТЕМАХ	312
Скоринович Б., Кулик Ю., Гавриляк В. АНАЛІЗ БЕЗПЕКИ ПІДХОДУ “ІНФРАСТРУКТУРА ЯК КОД” (INFRASTRUCTURE AS CODE) В ХМАРНИХ ОБЧИСЛЕННЯХ	318
Дорогий Я., Цуркан В., Дорога-Іванюк О. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ЗАХИСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УСТАНОВ ОСВІТНЬОЇ ГАЛУЗІ	323
Бердиченко І., Дорогий Я., Дорога-Іванюк О. ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ ЗАКОНОДАВСТВА ЄС ДЛЯ ЕФЕКТИВНОГО ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ ...	325
Сороченко М., Лаврик Т. БЕЗПЕКА БЛОКЧЕЙН: АНАЛІЗ АТАК ТА ВРАЗЛИВОСТЕЙ	330
Тулвїнський С. КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ПРИНЦИП ФУНКЦІОНУВАННЯ ПІДРОЗДІЛУ	332
Коробейнікова Т., Бодак А., Бороденко Д. НУЛЬОВА ДОВІРА: ПРИНЦИПИ, ВИКЛИКИ ТА ВПРОВАДЖЕННЯ	335
Токар В., Лучик В. РОЛЬ НАВЧАННЯ СПІВРОБІТНИКІВ У ЗАПОБІГАННІ КІБЕРАТАКАМ	340
Помаза-Пономаренко А., Тарадуда Д. КІБЕРБЕЗПЕКА ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	343
Щербина А. КІБЕРБЕЗПЕКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: СУЧАСНІ ВИКЛИКИ ТА РІШЕННЯ	347
Іщенко А., Марич В. ГІГ-КОНТРАКТ, ЯК ПРАВОВЕ ПОЛЕ З ОХОРОНИ ПРАЦІ ДЛЯ ПРАЦІВНИКІВ ІТ-КОМПАНІЙ	350
Яшук В., Мисько Р. ЗАХИСТ ОБ’ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ШЛЯХОМ ВПРОВАДЖЕННЯ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ	352
Дришлюк Д., Лучик В. МЕТОДИ РОЗСЛІДУВАННЯ ТА ДОКУМЕНТУВАННЯ КІБЕРАТАК НА ДЕРЖАВНІ УСТАНОВИ	355
Сафронов О., Лучик В. ВПЛИВ СУЧАСНИХ ЗАГРОЗ НА КІБЕРБЕЗПЕКУ ТА ЕФЕКТИВНІСТЬ ПІДХОДІВ ДО ЇХ ЗАПОБІГАННЯ ..	358
Сиротенко Б., Лучик В. ЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ	360
Шведов В., Рудик Ю. АПАРАТИ ЗАХИСТУ В СИСТЕМАХ SMART HOUSE	363
Кутняк М., Куперштейн Л. СИСТЕМА ОХОРОННОЇ СИГНАЛІЗАЦІЇ НА ОСНОВІ ПЛАТФОРМИ ARDUINO	366

**НАПРЯМ 8.
ІНФОРМАЦІЙНІ ВІЙНИ**

Кісіль Р. ФЕЙКОВІ НОВИНИ ЯК ІНСТРУМЕНТ СУЧАСНОГО ПРОТИСТОЯННЯ	370
Сабат В., Мацюк В. ФІШИНГ ЯК ЗАГРОЗА ОНЛАЙН СЕРЕДОВИЩА	373
Снапкова Н. РОЗУМІННЯ МАЙБУТНІМИ ОФІЦЕРАМИ ЗНАЧУЩОСТІ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНИ У ПРОЦЕСІ ЦИВІЛЬНО-ВІЙСЬКОВОЇ ВЗАЄМОДІЇ	377
Сікора Л., Рудько Д. ІНФОРМАЦІЙНІ АТАКИ НА СОЦІАЛЬНІ МЕРЕЖІ	382

СЕКЦІЯ 2

**ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ В УМОВАХ ВІЙНИ**

**НАПРЯМ 9.
ПРИКЛАДНЕ ТА СИСТЕМНЕ ПРОГРАМУВАННЯ**

Milianets T., Pukach A. SERVER LOAD BALANCING MATHEMATICAL MODEL BASED ON AUTOMATIC NODE'S RATING EVALUATION	387
Vilyk V. SURVEY OF DSL GENERATORS FOR THE JAVA PLATFORM	390
Кісіль О. РОЗРОБЛЕННЯ ПРОГРАМНОЇ СИСТЕМИ ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ СИЛ ТА ЗАСОБІВ ДЛЯ ГАСІННЯ ПОЖЕЖИ В ФОРМАТІ ЧАТ-БОТА	393
Літовська О. ДОСЛІДЖЕННЯ МЕТОДІВ ОБРОБКИ СИГНАЛУ RFG ДЛЯ ВИЯВЛЕННЯ ТА УСУНЕННЯ ВИКИДІВ	394
Павлюк О., Заболотна А., Міщук М. СИСТЕМА ЗБОРУ ТА ПРЕПРОЦЕСИНГУ ДАНИХ ТРИОСЬОВИХ АКСЕЛЕРОМЕТРА ТА ПІРОСКОПА ОТРИМАНИХ ЗА ДОПОМОГОЮ СМАРТ-ГОДИННИКІВ	399

Шопський О., Малець І. АНАЛІЗ І ВДОСКОНАЛЕННЯ МОДЕЛІ КЛАСТЕРИЗАЦІЇ ДАНИХ ДЛЯ ФОРМУВАННЯ ВИБІРКИ З МЕТОЮ ПРОГНОЗУВАННЯ РИЗИКОВИХ СИТУАЦІЙ	404
Ровецький І. АРХІТЕКТУРНІ ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ПРОГРАМНИХ СЕРВІСІВ З ПАРАЛЕЛЬНИМИ ОБЧИСЛЕННЯМИ .	407
Малець Б., Заблоцький Т. СИСТЕМА АНАЛІЗУ ДАНИХ ДЛЯ КУРСУ “МОДЕЛІ СТАТИСТИЧНОГО НАВЧАННЯ”	409
Мотульський В., Хлевной О. ОНЛАЙН-СЕРВІС ДЛЯ ОПЕРАТИВНОГО РОЗРАХУНКУ СИЛ ТА ЗАСОБІВ ПОЖЕЖНО-РЯТУВАЛЬНИХ СЛУЖБ У ЖИТЛОВИХ БУДИНКАХ ПІДВИЩЕНОЇ ПОВЕРХОВОСТІ	412
Либа О., Головатий Р. СИСТЕМА БРОНЮВАННЯ ЖИТЛА ДЛЯ ВОЛОНТЕРІВ	414
Поглод П., Смотров О. СТВОРЕННЯ ІНТЕГРОВАНОЇ МОБІЛЬНОЇ СИСТЕМИ ДЛЯ КООРДИНАЦІЇ ГУМАНІТАРНОЇ ДОПОМОГИ ТА ЕВАКУАЦІЙНИХ ЗАХОДІВ	417
Гапанович В., Смотров О. РОЗРОБКА МОБІЛЬНОГО СЕРВІСУ НАДАННЯ ПСИХОЛОГІЧНОЇ ДОПОМОГИ	420
Близиюк Т. РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СТВОРЕННЯ ПОРТАЛУ АВТОСПОРТИВНИХ НОВИН	423
Шпак З., Шувар М. ПАНЕЛЬ КЕРУВАННЯ ДЛЯ СИСТЕМИ РОЗУМНОГО БУДИНКУ НА БАЗІ ЧАТ-БОТУ МЕСЕНДЖЕРА	426

НАПРЯМ 10.

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Білик О., Мартинчук О. ВИЯВЛЕННЯ БПЛА ЗА ДОПОМОГОЮ SDR HACKRF ONE	430
Гнатюк В., Горбачов І. АНАЛІЗ СУЧАСНИХ ПРОГРАМНО-АПАРАТНИХ РІШЕНЬ ДЛЯ ІР-ТЕЛЕФОНІЇ	433
Гнатюк В., Батрак О., Головань М. МЕТОДИ ОПТИМІЗАЦІЇ РОБОТИ КОНТАКТ ЦЕНТРУ	437
Гамрецький Р., Гнатюк В. ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ І МОДЕЛЕЙ ОЦІНКИ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ	440
Паньків Т., Борзов Ю. РОЗРОБЛЕННЯ СЕРВІСУ ПОШУКУ НАЙБЛИЖЧИХ МЕДЗАКЛАДІВ НА ОСНОВІ ГЕОЛОКАЦІЇ	444
Громик О. АВТОМАТИЗАЦІЯ В РЕСТОРАННОМУ БІЗНЕСІ: СУЧАСНІ РІШЕННЯ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ТА СЕРВІСУ	447

Островерхий В., Молошний В. ВДОСКОНАЛЕННЯ УПРАВЛІННЯ КОМП'ЮТЕРНОЮ МЕРЕЖЕЮ ІНТЕРНЕТ ПРОВАЙДЕРА	451
Пилипенко В., Борзов Ю. ФУНКЦІОНУВАННЯ ЗАСОБІВ (СИСТЕМ) ЗВ'ЯЗКУ В ОРГАНАХ ТА ПІДРОЗДІЛАХ ДСНС УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ	453

НАПРЯМ 11.

3D МОДЕЛЮВАННЯ ТА 3D ДРУК

Духнич Н., Хлевной О. 3D МОДЕЛЮВАННЯ ТА 3D ДРУК – МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ	457
Івановський М., Кусій М. ВИКОРИСТАННЯ UNITY ДЛЯ 3D-МОДЕЛЮВАННЯ З ЕЛЕМЕНТАМИ ЛІНІЙНОГО ШИФРУВАННЯ	460
Довбняк В. АКТУАЛЬНІСТЬ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ 3D-ВІЗУАЛІЗАЦІЇ У ПРОФЕСІЙНІЙ ПІДГОТОВЦІ МАЙБУТНІХ ФАХІВЦІВ	464

НАПРЯМ 12.

МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СИСТЕМ

Semenyuk S. APPLICATION OF THE STOCHASTIC SIR MODEL TO CYBERSECURITY THREATS MODELING	466
Гембара Т. ІДЕНТИФІКАЦІЯ НЕПЕРЕВНИХ АКУСТИЧНИХ СИГНАЛІВ МАТЕМАТИЧНИМИ МЕТОДАМИ ДИСКРЕТИЗАЦІЇ ІНТЕГРАЛЬНИМИ ПЕРЕТВОРЕННЯМИ	470
Льків А., Борзов Ю. РОЗРОБКА ПРОГРАМНОГО СЕРВІСУ ВИЗНАЧЕННЯ РІВНЯ ЗАБРУДНЕНЬ ПОВІТРЯ НА ДІЛЯНЦІ ДОРОГИ	474
Кудряшова А., Петрик В. СЕМАНТИЧНА МЕРЕЖА ФАКТОРІВ ВПЛИВУ НА ЯКІСТЬ ОБРОБЛЕННЯ КНИЖКОВИХ БЛОКІВ	478
Піх І., Михайлович Н. ОПТИМІЗАЦІЯ МЕТОДІВ ПОПЕРЕДНЬОЇ ОБРОБКИ ТА АУГМЕНТАЦІЇ ДАНИХ ДЛЯ НЕЙРОННИХ МЕРЕЖ У МЕДИЧНІЙ ВІЗУАЛІЗАЦІЇ ЛЕГЕНЬ	482
Літнік М., Назар Ю. МОДЕЛЬНО-ОРІЄНТОВАНИЙ ПІДХІД ДО АВТОМАТИЗАЦІЇ ГЕНЕРАЦІЇ ТЕСТОВИХ ВИПАДКІВ НА ОСНОВІ UML ДІАГРАМ	486
Верхола М. МОДЕЛЮВАННЯ ТА АНАЛІЗ ПРОЦЕСУ ОФСЕТНОГО ДРУКУ	490
Гавриць А., Філіппова В. ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ARCGIS PRO В СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ	495

Котелович Д., Борзов Ю. НАВЧАННЯ РОБОТІВ БАЛАНСУВАТИ: ДОСЯГНЕННЯ ТА ПРОБЛЕМИ	498
Мельник М., Рудик Ю. АЛГОРИТМІЗАЦІЯ РОЗРАХУНКУ ПАРАМЕТРІВ ЗАХИСНИХ ГІДРОТЕХНІЧНИХ СПОРУД	501

НАПРЯМ 13.

ОРГАНІЗАЦІЯ БАЗ ДАНИХ І ЗНАТЬ

Захаренко В. ФОРМУВАННЯ ОБЛІКУ СХОВИЩА ДАНИХ ДЛЯ ОБЛІКУ ТРАНЗАКЦІЙ ПРОІЗДІВ У МІСЬКОМУ ТРАНСПОРТІ ...	505
Придатко О., Гащук Л., Гащук П. ІДЕНТИФІКАТОРИ СТРУКТУРНИХ І РЕЖИМНИХ ВЛАСТИВОСТЕЙ АВТОМОБІЛЬНИХ МАРШРУТІВ	509
Мусянович М., Райта Д. СИСТЕМА ТЕЛЕФОННОЇ КНИГИ ДЛЯ УНІВЕРСИТЕТУ	514
Придатко О., Гащук Л., Гащук П. ПРИНЦИП РОБОТИ БАЗ ДАНИХ ЗА МОДЕЛЛЮ КЛЮЧА ТА ЗАМКА	516

НАПРЯМ 14.

ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ ДАНИХ

Hibey P., Sabat V. ENHANCING VIDEO SEARCH WITH MULTI-MODAL LLM AND VECTOR EMBEDDING TECHNIQUES	519
Мицишин О. ПРОБЛЕМИ МОДЕЛЮВАННЯ ТА ВІЗУАЛІЗАЦІЇ СОЦІАЛЬНО-ЕКОНОМІЧНИХ ПРОЦЕСІВ	521
Жуков Д., Ровецький І. ДОСЛІДЖЕННЯ ВПЛИВУ ЗОВНІШНІХ ФАКТОРІВ НА ЯКІСТЬ ЗВ'ЯЗКУ З БЕЗПЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ В УМОВАХ ОПЕРАТИВНИХ ДІЙ	525
Латишевч С. РОЗПІЗНАВАННЯ ЗГЕНЕРОВАНИХ ШТУЧНИМ ІНТЕЛЕКТОМ ЗОБРАЖЕНЬ АБО ВІДЕО МАТЕРІАЛІВ	527
Давидкін М. АНАЛІЗ МЕТОДІВ КОМП'ЮТЕРНОГО ЗОРУ ДЛЯ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ	530
Качур Р. АНАЛІЗ МЕТОДІВ ІНТЕРПОЛЯЦІЇ ЗНАЧЕНЬ КЛЮЧОВИХ КАДРІВ У КОМП'ЮТЕРНІЙ АНІМАЦІЇ	533

НАПРЯМ 15.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРОЄКТАМИ

Pukach A., Teslyuk V. SUBJECTIVE PERCEPTION MODEL OF SOFTWARE SUPPORT, ENCAPSULATED WITH A MULTILAYER PERCEPTRON	538
---	-----

Kovalchuk O., Ratushnyi R., Peretyatko L., Zhuk I. RISK MANAGEMENT OF CYBER PROTECTION PROGRAMS FOR CRITICAL INFRASTRUCTURE FACILITIES	542
Мідянка В. ПРОЕКТУВАННЯ ІНТЕРАКТИВНОЇ СИСТЕМИ УПРАВЛІННЯ ГОТЕЛЬНИМ БІЗНЕСОМ ЗА ДОПОМОГОЮ UML-ДІАГРАМ	546
Деліжан І., Соколова Є. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ОБЛІКУ ПРОЄКТНОЇ ДІЯЛЬНОСТІ	550
Мечус Х., Смотр О. ВПЛИВ СОЦІАЛЬНИХ МЕРЕЖ НА ОСВІТНІЙ ПРОЦЕС: АНАЛІЗ ДАНИХ ЗА ДОПОМОГОЮ БІБЛІОТЕК RUTNOM	554
Малець І., Горностаї Ю. “РОЗУМНА ПОЖЕЖНА ЧАСТИНА” – ІННОВАЦІЙНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ	558
Мудрак В. ЦИФРОВІ РОБОЧІ МІСЦЯ ЯК АЛЬТЕРНАТИВА ТРУДОВІЙ МІГРАЦІЇ	560
Перетятко Л., Стеців І. УПРАВЛІННЯ РИЗИКАМИ В ІТ-ПРОЄКТАХ	563
Перетятко Л., Дубиницька П. ВИКОРИСТАННЯ ЦИФРОВИХ ІНСТРУМЕНТІВ ТА ТЕХНОЛОГІЙ ДЛЯ УПРАВЛІННЯ КОМАНДОЮ	566

НАПРЯМ 16.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Venherskyi P., Bolishchuk S., Oskirko M., Peleshko D. SAFE INTEGRATION OF THE LANGUAGE MODEL OF ARTIFICIAL INTELLIGENCE IN AN INTERACTIVE SUPPORT SCENARIO TRAINING CLASSES IN REAL TIME. VULNERABILITIES AND RISKS IN USING APPLYING AI MODELS	569
Дубина В. АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ І ЗАСОБІВ КІБЕРБЕЗПЕКИ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ УКРАЇНИ	573
Мудровський Р. ДОПОВНЕНА ТА ВІРТУАЛЬНА РЕАЛЬНІСТЬ У НАВЧАЛЬНОМУ ПРОЦЕСІ ПОЛЩЕЙСЬКИХ	576
Гарань П., Головатий Р. ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ПРОЗОРОСТІ У НАУКОВИХ РЕПОЗИТОРІЯХ УНІВЕРСИТЕТІВ	578
Левко О., Головатий Р. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ: СУЧАСНІ МОЖЛИВОСТІ ТА ВИКЛИКИ	581
Бурак Н., Яковчук В. ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ РУШІЯ UNITY ДЛЯ СТВОРЕННЯ ІГРОВИХ ВІЗУАЛІЗАЦІЙ ТА ЇХНЬОГО ВПЛИВУ НА ЕФЕКТИВНІСТЬ НАВЧАННЯ	584
Дзень В., Борзов Ю., Дзень Д. ІНТЕГРАЦІЯ SMART-СИСТЕМ В ОСВІТНЄ СЕРЕДОВИЩЕ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ	587

Андрухів Д., Кобко Є., Придатко О. ІНФОРМАЦІЙНІ СИСТЕМИ УПРАВЛІННЯ ОСВІТНІМ ПРОЦЕСОМ, АРХІТЕКТУРА ТА ОПТИМІЗАЦІЯ ЗА ДОПОМОГОЮ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ..	589
Оскерко С., Малець І. ПОТЕНЦІАЛ ЗАСТОСУВАННЯ FDM ДРУКУ В ОСВІТНЬОМУ ПРОЦЕСІ	594
Ільчук Д. КІБЕРБЕЗПЕКА ДІТЕЙ ТА МОЛОДІ: ПРОФІЛАКТИКА ТА ОСВІТА	597
Лучик В., Журавель В. ВПЛИВ КІБЕРЗАГРОЗ НА МОРАЛЬНИЙ СТАН НАСЕЛЕННЯ	600
Запогічна Р. СУЧАСНІ ІНТЕРАКТИВНІ МЕТОДИ ЕФЕКТИВНОГО ВИВЧЕННЯ ІНОЗЕМНОЇ МОВИ ЗДОБУВАЧАМИ ВИЩОЇ ОСВІТИ ПРОГРАМИ “ПРАВООХОРОННІ ІНФОРМАЦІЙНІ СИСТЕМИ”	603
Кучаковська Г. ПРОФЕСІЙНА ПІДГОТОВКА ВЧИТЕЛІВ ПОЧАТКОВОЇ ШКОЛИ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА (ЄВРОПЕЙСЬКИЙ ДОСВІД)	607
Харчук А., Воробйов О. ПЕДАГОГІЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ ПІД ЧАС ВІЙСЬКОВОЇ АГРЕСІЇ	611
Павловська Д., Пархоменко Р. ВІРТУАЛЬНІ СИМУЛЯТОРИ ДЛЯ НАВЧАННЯ ПРАВИЛАМ ЕВАКУАЦІЇ	613
Муха І., Пархоменко В.-П., Пархоменко Р. ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ НАВЧАННЯ ПОЖЕЖНИЙ БЕЗПЕЦІ	617
Альфавіцька Г., Пархоменко В.-П., Пархоменко Р. ЦИФРОВІЗАЦІЯ ПРОГРАМ НАВЧАННЯ ДЛЯ ПОЖЕЖНИХ-РЯТУВАЛЬНИКІВ	619

Наукове видання

**ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-
КОМУНІКАЦІЙНИХ СИСТЕМАХ**

Збірник наукових праць
V Міжнародної науково-практичної конференції
ІБІТ 2024

Відповідальні за випуск

Ростислав ТКАЧУК

Оригінал-макет

Ростислав ТКАЧУК

Друк на різнографі

Підписано до друку 13.12.2024 р.
Формат 70×100/16. Гарнітура Times New Roman.
Папір офсетний. Друк цифровий.
Ум. друк. арк. 51,68. Обл.-вид. арк. 46,71
Наклад 100 прим.

Видавець і виготовлювач: ТОВ «Растр-7»
79005, м. Львів, вул. Кн. Романа, 9/1.
Тел./факс: (032) 235 72 13. E-mail: rastr.sim@gmail.com
www.rastr-7.com.ua

Свідоцтво суб'єкта видавничої справи
ЛВ № 22 від 19.11.2002 р.



**V International Scientific and Practical
Conference CYBERSUCURITY AND
INFORMATION TECHNOLOGY
CIT 2024**

November 27 - 2024 Lviv-Ukraine