НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

Редакційна колегія:

ГОРБАЧЕНКО Станіслав, д.е.н., професор

СОКОЛОВ Артем, д.т.н., професор

АХМАМЕТЬЄВА Ганна, к.т.н., доцент

РАЗІНКІН Нікіта, асистент кафедри

© НУ «Одеська юридична академія», 2025

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies, Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material bears the participants of the conference, their scientific supervisors, who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

Editorial Board:

GORBACHENKO Stanislav, Doctor of Economics, Professor

SOKOLOV Artem, Doctor of Engineering, Professor

AKHMAMETYEVA Anna, Candidate of Engineering, Associate Professor

RAZINKIN Nikita, Assistant

© National University "Odesa Law Academy", 2025

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

Шановні учасники щорічної Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики»!

Сьогодні, в умовах триваючої повномасштабної війни, як ніколи важливо усвідомлювати роль кібербезпеки. Кіберпростір, який раніше сприймався переважно як технічний інструмент чи канал обміну інформацією, перетворився на стратегічну арену, де інформаційні впливи та технологічні рішення визначають майбутнє безпеки, управління та соціального розвитку. Нові загрози національній безпеці все частіше пов'язані зі стрімким розвитком технологій. Для ефективній протидії цим викликам необхідна консолідація знань, інноваційні підходи та міжнародне співробітництво.

У сучасних умовах ми стикаємося з новими, нетиповими загрозами національній і глобальній безпеці, від стрімких технологічних трансформацій та кібератак на критично важливі інфраструктури до порушень інформаційних прав людини та поширення дезінформації, здатної підірвати довіру до державних інституцій та суспільних цінностей. Ця багатовимірність викликів робить очевидним, що кібербезпека вже давно перестала бути лише технічною проблемою. Вона стала справжньою мультидисциплінарною сферою знань, де для ефективного захисту необхідні наукові результати та експертиза як із технічних наук: інженерії, комп'ютерних технологій, криптографії, так і з гуманітарних та соціальних дисциплін: права, економіки, психології, соціології та управління.

Адаптація до нових реалій війни та глобальних викликів XXI століття вимагає консолідації міжнародних зусиль і розвитку міждисциплінарних досліджень. Від технічних фахівців, що розробляють інноваційні протоколи захисту інформаційних систем, до юристів, які формують правові стандарти цифрового простору; від економістів, що оцінюють наслідки кібератак для бізнесу та держави, до психологів, що досліджують вплив кіберзагроз на свідомість людей. Усі вони повинні працювати як єдина команда. Лише така інтеграція знань та підходів дозволяє створити комплексну систему протидії викликам безмежного та динамічного кіберпростору.

Наше місто, Одеса, традиційно вирізняється потужним інтелектуальним, науковим та культурним потенціалом, а також динамічним IT-сектором. Національний університет «Одеська юридична академія» як впливовий центр науки і освіти створює унікальну платформу для об'єднання провідних дослідників і практиків із різних країн і галузей. На нашій конференції представлено здобутки науковців з України, Франції, Польщі, Сербії та Індії, які зробили величезний внесок у розвиток кібербезпеки та продовжують

залишатися на передньому краї наукового прогресу. Їхній досвід і новаторські ідеї формують стандарти, що визначають майбутнє захисту цифрового простору, а участь у конференції дозволяє учасникам з усього світу обмінюватися знаннями та створювати спільні інноваційні рішення для сучасних викликів кібербезпеки.

Ми сподіваємося, що цьогорічна конференція стане платформою для плідної співпраці, обміну знаннями, ідеями та досвідом як науковців, так і практиків, і сприятиме створенню ефективних рішень для захисту сучасного кіберпростору.

Президент Національного університету
“Одеська юридична академія”,
академік НАПрН України, академік НАПН України
доктор юридичних наук, професор,
Заслужений юрист України *Сергій КІВАЛОВ*

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ У СОЦІАЛЬНИХ МЕРЕЖАХ: ВИКЛИКИ ТА ЗАГРОЗИ СУЧАСНОГО ЕТАПУ

Дикий Олег

декан факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»,
кандидат юридичних наук, доцент

Проблематика забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах у 2025 році набула критичного значення у зв'язку з повномасштабною збройною агресією російської федерації проти України та трансформацією гібридної війни в широкомасштабне вторгнення, де інформаційний простір виступає одним із ключових театрів бойових дій. Соціальні інтернет-сервіси, які ще донедавна розглядалися переважно як інструмент комунікації та соціальної взаємодії, фактично перетворилися на системоутворюючий елемент національного інформаційного середовища, здатний безпосередньо впливати на суспільну свідомість, поведінку громадян і стабільність державних інституцій.

У цьому контексті вважаю, що положення, викладені у статті Р. Грищука та К. Молодецької-Гринчук «Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах», зберігають не лише наукову, а й значну прикладну цінність. Запропонована авторами методологія комплексного моніторингу текстового контенту, виявлення та оцінювання організаційних, змістовних і маніпулятивних ознак загроз, а також аналіз профілів акторів соціальних мереж повністю відповідає сучасному характеру інформаційних операцій, що реалізуються проти України[1].

Після 2022 року соціальні мережі та месенджери стали основним каналом поширення дезінформації, маніпулятивних наративів і психологічного тиску на населення. У матеріалах українських та міжнародних засобів масової інформації неодноразово фіксувалися приклади координованих кампаній у Telegram, Facebook та X (Twitter), спрямованих на дискредитацію Збройних Сил України, підрив довіри до процесів мобілізації, формування панічних настроїв та спотворення інформації про міжнародну підтримку України. Такі кампанії, як правило, характеризуються використанням бот-мереж, псевдоекспертних коментарів, емоційно забарвленого контенту та прихованих семантичних конструкцій, що є механізмами інформаційно-психологічного впливу.

Варто звернути увагу, що соціальні інтернет-сервіси є складними соціотехнічними системами з нелінійною динамікою розвитку. В умовах війни

українське суспільство перебуває у стані підвищеної інформаційної напруги, коли навіть незначні інформаційні імпульси можуть призводити до різких соціальних коливань. Це підтверджує доцільність використання елементів теорії динамічного хаосу, біфуркацій і атракторів для аналізу поведінки віртуальних спільнот, що дозволяє адекватніше описувати процеси переходу від стабільного до нестійкого стану інформаційної безпеки.

Не менш актуальною є концепція синергетичного управління, запропонована у статті[1], яка передбачає використання природних механізмів самоорганізації акторів соціальних мереж для досягнення керованого переходу віртуальних спільнот до заданого стійкого стану інформаційної безпеки. Такий підхід корелює з положеннями, викладеними у працях В. Горбуліна, О. Додонова та Д. Ланде, де інформаційні операції розглядаються як системний інструмент впливу на безпеку суспільства та держави, а протидія їм потребує комплексних міждисциплінарних рішень[2].

У зв'язку з цим постає низка наукових питань, що потребують подальшого системного дослідження. Передусім це проблема своєчасного виявлення моментів переходу інформаційного середовища соціальних інтернет-сервісів у критичний або передкризовий стан, коли локальні інформаційні впливи здатні спричиняти масштабні соціальні ефекти. Недостатньо вивченими залишаються закономірності формування та еволюції деструктивних інформаційних наративів, механізми їх адаптації до змін зовнішнього контексту та способи інтеграції таких наративів у природні комунікаційні потоки віртуальних спільнот.

Окремої уваги потребує дослідження ролі автоматизованих та напівавтоматизованих акторів, зокрема бот-мереж і керованих акаунтів, у процесах штучного підсилення інформаційних коливань. Актуальним є також питання ідентифікації прихованих центрів управління інформаційними кампаніями, а також визначення критеріїв відмежування органічної громадської дискусії від скоординованого інформаційно-психологічного впливу. У цьому контексті важливим напрямом подальших досліджень є розроблення показників стійкості віртуальних спільнот до дезінформаційних впливів та методів оцінювання ефективності контрнаративів.

З методологічної точки зору доцільним видається використання міждисциплінарного підходу, що поєднує системний аналіз, методи теорії складних систем, соціальної інформатики та кібернетики. Перспективним є застосування математичного моделювання нелінійних процесів у соціальних інтернет-сервісах у поєднанні з емпіричним аналізом великих масивів даних, отриманих у результаті моніторингу відкритих джерел. Такий підхід дозволяє не лише фіксувати вже реалізовані інформаційні атаки, але й прогнозувати можливі сценарії розвитку інформаційних загроз.

Крім того, подальшого розвитку потребують методи синергетичного управління інформаційною безпекою, спрямовані на використання внутрішніх механізмів самоорганізації віртуальних спільнот. Йдеться про формування умов, за яких деструктивні інформаційні впливи втрачають здатність до масштабування, а система повертається до відносно стійкого стану без застосування надмірних адміністративних або репресивних заходів. У поєднанні з сучасними інструментами аналізу природної мови, мережевої аналітики та елементами штучного інтелекту така методологія може стати основою для побудови ефективних систем забезпечення інформаційної безпеки держави в умовах тривалої війни.

Список використаних джерел

1. Грищук Р., Молодецька-Гринчук К. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах // Захист інформації. – 2017. – Т. 19, № 4 (жовтень–грудень). – С. 254–262. – DOI: 10.18372/2410-7840.19.12204.
2. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. – Київ : Інтертехнологія, 2009. – 164 с.

Ключові слова: інформаційна безпека держави, соціальні інтернет-сервіси, дезінформація, інформаційно-психологічний вплив.
Keywords: state information security, social internet services, disinformation, information and psychological influence.

A REVIEW ON MANY-VALUED LOGIC: A NOVEL PARADIGM FOR INFORMATION SECURITY

Aboobacker P
Govt.Engineering College, Palakkad, India
Department of Mathematics, Ph.D., Assistant Professor

1. Introduction. In the modern world, technology is changing at an astounding rate. We are more inventive, efficient, and connected than ever. Although this digital revolution has opened up a lot of possibilities, it has also increased risk and complexity. This scenario includes two phases: the incredible opportunity the digital world offers us and the significant challenges we must all overcome to realize that potential.

Modern advancement is built upon connectivity. Cybersecurity is not an obstacle to innovation; rather, it is a crucial enabler that permits us to safely seize new opportunities. The Internet has become the fastest-growing daily infrastructure. Many current technological advancements are transforming society. However, these new

technologies often lack adequate safeguards for personal data, leading to an increase in cybercrimes.

Cybersecurity is the silent, foundational infrastructure for all digital advancement. The digital world relies entirely on this trust and safety; without it, progress stops. The core challenge is simple: as connectivity increases opportunities, it simultaneously expands vulnerabilities, requiring a stronger security foundation to support a more complex world.

2. Cryptography and Cyber security. The fields of communication and cybersecurity are inherently connected. The goal of cybersecurity is to safeguard communication systems and the information they carry, while robust communication is essential for creating, maintaining, and addressing security risks. Strong secure communication is required by the fast-growing interconnection of the entire universe.

Cryptography, the study and application of methods for safe communication and data security against adversaries, is one of the solutions against exploitation in this setting. Encryption is the process of employing mathematical ideas to convert readable data (plaintext) into an unintelligible format (ciphertext) that can only be decoded by the intended recipients. Encryption is an essential and crucial feature of cybersecurity, mainly because it makes sure that data is unreadable even if it is accessed by unauthorized people. It supports a number of important security concepts, such as integrity, confidentiality, and authentication. While cryptography focuses on security, cryptanalysis addresses attack defensive mechanisms.

3. Moving Beyond Binary Choices. The fundamental problem and principle of contemporary cybersecurity research is that current security models are frequently inadequate against changing threats, calling for creative, multi-layered solutions and the creation of new paradigms that go beyond conventional methods. One approach involves moving beyond traditional binary systems to develop methods and systems based on many-valued logic, (MVL) which offers a potential foundation for creating novel and enhanced cryptographic algorithms. Unlike classical two-valued logic—where a statement is strictly true (1) or false (0)—MVL systems incorporate additional truth values (ternary, quaternary, fuzzy logic etc.). This expanded framework provides the capacity to effectively model uncertainty, imprecision, and more complex relationships within computational and security systems.

Benefits of Many-Valued Logic in Cryptography:

– **Compact data representation:** Many-valued logic systems store and analyze more **information per unit**. For instance, with equivalent hardware or the same digit count, a ternary system holds more information per trit than a binary system due to its inherently higher data representation density. This dense processing capability allows custom hardware implementations to potentially achieve better performance while consuming less power.

– **Complex Algorithms with potential:** Incorporating many-valued functions into cryptographic primitives significantly increases their complexity, enhancing security. This approach is fundamental for designing robust components as it elevates the difficulty of solving the underlying mathematical problems faced by attackers.

– **Advanced Algorithmic Methodologies and Optimized Performance:** By implementing MVL number systems like residue and redundant systems, arithmetic operations can be speed up by reducing or eliminating the carry propagation, a key benefit for resource-constrained environments. This capability also facilitates the development of novel, high-quality algorithms. These new algorithms leverage unique properties to offer better statistical parameters, including enhanced nonlinearity and non-correlation than some existing binary based algorithms.

– **Hardware Optimization:** MVL allows designers to reduce both the transistor count and the number of physical connections, which results in Compact, performance-optimized devices.

Disadvantages of Many-Valued Logic in Cryptography:

– **Incompatibility with Binary Infrastructure:** Since most existing computer infrastructure operates exclusively on binary logic, integrating MVL algorithms requires custom hardware or complex software adaptation. This leads to significant difficulty to both the design process and ongoing management.

– **Limited Maturity and Resources:** Compared to classical binary cryptography, the field of MVL cryptography is less developed and lacks standardized protocols. The limited availability of existing research and specialized expertise creates significant hurdles for both development and testing.

– **The changing threat landscape and Limited Research:** The adoption of new logical approaches and nascent circuit systems introduces the risk of novel, previously unstudied vulnerabilities that could be exploited by malicious actors. Furthermore, the limited research into cryptanalysis methods specifically targeting MVL systems makes it challenging to thoroughly evaluate and guarantee the long-term security of these new algorithms compared to established, battle-tested binary ones.

Conclusion. The digital revolution offers extensive opportunities but necessitates a strong security basis as increased connectivity also broadens vulnerabilities. Cryptography is crucial for securing communication and protecting data, with many-valued logic (MVL) proposing a shift from binary systems to develop more complex algorithms. This method could enhance hardware efficiency and cryptographic strength, although challenges persist such as incompatibility with current binary systems, lack of standards, and potential unstudied vulnerabilities. Therefore, despite its promise for future security progress, practical obstacles must be resolved before MVL can be widely adopted.

References:

1. Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity, 7(1), tyab005.
2. Stallings, W. Cryptography and Network Security - Principles and Practice.
3. I F. Volynets-Velikorodov and M. S. Klimash. Prospects for the Application of Many-Valued Logic Functions in Cryptography Proceedings of the 2018 IEEE 4th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD).

Ключові слова: кібербезпека, криптографія, багатозначна логіка.
Keywords: cybersecurity, cryptography, many-valued logic.

МЕТОДИ ТА РИЗИКИ ПОБУДОВИ СИСТЕМ З END-TO-END ШИФРУВАННЯМ

Вінковська Ірина

Національний університет «Одеська політехніка»,
старший викладач кафедри кібербезпеки та програмного забезпечення

Чебаненко Олег

Національний університет «Одеська політехніка»,
студент кафедри кібербезпеки та програмного забезпечення

Вступ. Сучасні інформаційні технології забезпечують швидкий обмін даними між користувачами через різноманітні месенджери (Telegram, WhatsApp, Signal тощо). Проте зростання кількості кіберзагроз робить актуальною проблему забезпечення конфіденційності та цілісності повідомлень. Більшість популярних месенджерів використовують власні протоколи шифрування, але їхній вихідний код або архітектура не завжди відкриті для аудиту, що створює ризики втрати контролю над безпекою даних.

У зв'язку з цим постає завдання створення відкритих програмних рішень, які реалізують принцип end-to-end шифрування (E2EE) – коли лише відправник і отримувач мають доступ до змісту повідомлень, а сервер виконує лише роль транспортного посередника.

Мета: Проаналізувати сучасні підходи до реалізації end-to-end шифрування в месенджерах та визначити напрями створення програмного застосунку, який забезпечить конфіденційність, цілісність і автентичність повідомлень під час обміну даними між користувачами.

Проблематика захищеного обміну повідомленнями

Передача даних у мережах часто супроводжується ризиками несанкціонованого доступу, підміни або перехоплення повідомлень.

Уразливими є системи, що не застосовують повноцінного шифрування або використовують слабкі алгоритми. Проблемою також є централізоване зберігання ключів на сервері, що створює можливість їх компрометації.

Багато месенджерів не мають прозорих механізмів обміну ключами, що знижує рівень довіри користувачів і не гарантує повної конфіденційності даних. Тому, створення незалежної клієнтської системи шифруванням є важливою передумовою для підвищення рівня безпеки комунікацій [1].

Методи криптографічного захисту

Основою безпечного обміну даними є асиметричне шифрування, де кожен користувач має пару ключів – відкритий і закритий. У межах дослідження розглядаються алгоритми RSA та ElGamal, які дозволяють здійснювати безпечну передачу даних без необхідності обміну секретними ключами.

Алгоритм RSA ґрунтується на складності факторизації великих чисел. Для роботи генеруються два великі прости числа, на основі яких формується пара ключів: відкритий для шифрування, закритий – для розшифрування.

Алгоритм ElGamal базується на складності обчислення дискретного логарифма, і який створює унікальний шифр текст при кожному шифрування одного й того ж повідомлення [2].

Для забезпечення цілісності даних буде використовуватись криптографічна хеш-функція SHA-256, що перетворює повідомлення на фіксований 256-бітний хеш.

Автентифікація користувачів та підтвердження походження даних забезпечуватимуться за допомогою цифрових підписів, які формуються шляхом шифрування хешу повідомлення закритим ключем відправника [3].

Поєднання асиметричного шифрування (RSA та ElGamal), хешування (SHA-256) та цифрових підписів забезпечить комплексний, багаторівневий захист повідомлень і повну відповідність принципу end-to-end шифрування.

Аналіз проблем та ризиків при побудові месенджера end-to-end шифрування

Під час створення месенджера з end-to-end шифруванням однією з основних проблем є забезпечення захищеного обміну відкритими ключами. У разі їх підміни можливі атаки типу «людина посередині», що дозволяє зловмиснику читати або змінювати повідомлення. Додатковим ризиком є компрометація приватного ключа на пристрої користувача, що відкриває доступ до всієї історії переписки.

Важливою загрозою залишається верифікація автентичності користувачів: навіть при коректній криптографічній реалізації система може бути вразливою до соціальної інженерії або підроблених ключів. Уразливість також виникає під час зберігання локальних даних – зараження пристрою шкідливим ПЗ може призвести до витоку інформації до її шифрування.

Технічні ризики пов'язані з керування ключами та сесіями, неправильним оновленням криптографічного матеріалу та відсутністю механізмів forward secrecy. Навіть за відсутності доступу до відкритих даних компрометація серверної інфраструктури може вплинути на доставку повідомлень і цілісність ключів. Тому побудова безпечного месенджера потребує комплексного підходу, що враховує криптографічні, мережеві та користувацькі ризики.

Висновок. Розробка месенджера з end-to-end шифруванням є актуальним завданням кібербезпеки для захисту даних. Ефективна реалізація E2EE вимагає надійних криптоалгоритмів, безпечного обміну ключами, захисту клієнтських пристроїв та перевірки належної автентифікації. Поєднання RSA, ElGamal, SHA-256 та цифрових підписів створює багаторівневий захист від сучасних загроз. У планах – створення програмного застосунку для практичної демонстрації та підтвердження ефективності цих методів.

Перелік використаних джерел:

1. Наскрізне шифрування: що це таке та як працює. – URL: https://root-nation.com/ua/articles-ua/tech-ua/ua-end-to-end-encryption/
2. Яремчук Ю.Є., Салієва О.В., Бондаренко І.О. Основи криптографічного захисту інформації. – URL: https://pdf.lib.vntu.edu.ua/books/2024/Yaremchuk_2024_139.pdf
3. Що таке криптографія у блокчейні. 2025. – URL: https://www.web3.org.ua/shcho-take-kryptohrafiia-u-blokchejni/

Ключові слова: end-to-end шифрування, RSA, ElGamal, SHA-256, цифровий підпис.
Key words: end-to-end encryption, RSA, ElGamal, SHA-256, digital signature.

A 10-BIT S-BOX GENERATED BY FEISTEL CONSTRUCTION FROM CELLULAR AUTOMATA

Thomas Prévost
Université Côte d'Azur, France, I3S, Ph.D. student
Bruno Martin
Université Côte d'Azur, France, I3S,Ph.D., full professor

Abstract. In this paper, we propose a new 10-bit S-box generated from a Feistel construction. The subpermutations are generated by a 5-cell cellular automaton based on a unique well-chosen local transition rule and bijective affine transformations. In particular, the cellular automaton rule is chosen based on empirical tests of its ability to generate good pseudorandom output on a ring cellular

automaton. Similarly, Feistel network layout is based on empirical data regarding the quality of the output S-box.

Introduction. Symmetric cryptography is central to securing modern communication systems, enabling two parties that share a secret key to exchange information that appears indistinguishable from random data to any outside observer. Among symmetric techniques, block ciphers dominate practical applications, with algorithms such as AES and Blowfish setting the standard. A critical element in these designs is the substitution box (S-box), which introduces the nonlinearity necessary to resist a wide range of cryptanalytic attacks. Because attacks like linear, differential, and boomerang cryptanalysis typically exploit weaknesses in S-boxes, their careful design is essential.

The challenge lies in the immense design space: an n-bit S-box corresponds to a permutation of 2n elements, leading to a factorial explosion in the number of possible candidates. For commonly used sizes, such as 8-bit S-boxes in AES or the 10-bit S-box introduced in this work, the search space is far too large for exhaustive analysis. Consequently, most existing constructions rely on algebraic structures over finite fields to produce S-boxes with desirable security properties.

In contrast, this paper explores a combinatorial approach to S-box design. We construct a 10-bit S-box using an 11-round Feistel network composed of three affine bijective layers and eight permutation layers derived from a one-dimensional uniform binary cellular automaton. A carefully selected local Boolean function drives the cellular automaton, providing pseudo-random permutation behavior within the Feistel framework.

Uniform cellular automaton. Cellular automata (CA) are discrete, parallel computational models composed of cells that update their states synchronously according to a local rule based on their own state and those of their neighbors. A well-known example is Conway's Game of Life.

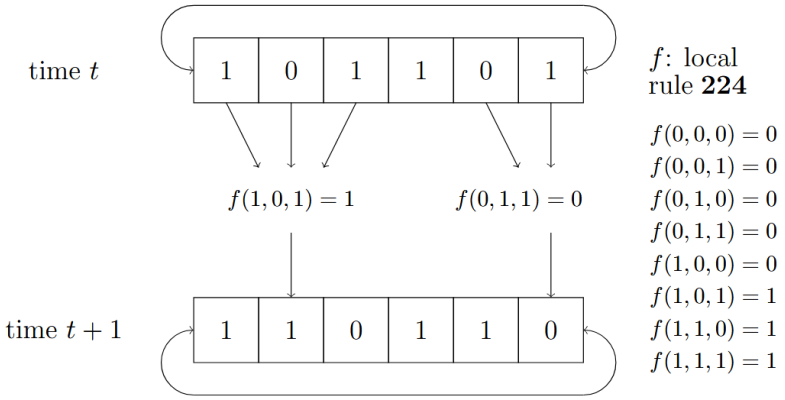

Figure 1: Example of a 1-dimensional uniform cellular automaton with the single 3-bit local rule 224. To compute the next value of a cell on the border, we consider the cell on the other edge as neighboring this one.

A 1-dimensional CA is defined by a triple (Q, δ, N) where Q is the set of states (here {0,1}), δ: Qn → Q is the local transition rule (a Boolean function of arity n), and N ⊆ ℤ is the neighborhood. We consider finite rings of Boolean cells, where edge cells take neighbors from the opposite side.

A CA is uniform if the same local rule is applied to every cell. With a suitable rule, uniform CAs can produce sequences with pseudo-random or chaotic behavior, as demonstrated for example by Wolfram's rule 30 [3]. They have been studied as potential pseudo-random bit generators, though LFSRs remain more common.

Uniform CAs can also exhibit short, non-chaotic cycles for certain inputs, such as uniform configurations, so care is required when using them in cryptographic settings.

Feistel networks.

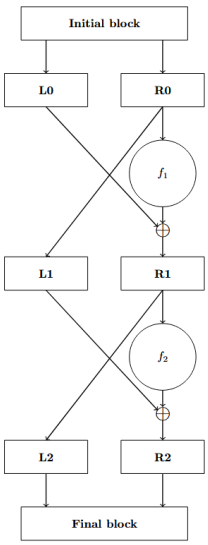

Figure 2: Example of Feistel construction of depth 2. f_1 and f_2 are pseudo-random permutations.

The Feistel network [1] provides a way to build pseudo-random bijective permutations from pseudo-random functions. When stacked in multiple rounds, the resulting network yields permutations that are computationally indistinguishable from random ones [2].

As illustrated in Fig. 2, an n-bit Feistel network splits the input into two halves and applies a sequence of round functions fi of size $\frac{n}{2}$. The number of such functions defines the network's depth.

Our 10-bit S-Box construction. To generate our 10-bit S-box, we evaluate a Feistel permutation on all 1024 inputs, ensuring bijectivity so the S-box can be inverted. Each round function f_i is either a 5-cell uniform cellular automaton (used as

a pseudo-random permutation) or an affine bijection $f_{a,b}(x) = ax + b mod 2^{10}$ with $\gcd(a, 2^{10}) = 1$.

Our Feistel network has 11 layers: an affine layer $f_{5,3} = 5x + 3 \bmod 1024$; four CA-based layers; an affine layer $f_{7,11}$; three CA layers; an affine layer $f_{13,17}$; one final CA layer.

To build the local CA permutation, we use a 5-cell ring updated once by a single 5-variable Boolean rule. We reduce the 2^{32} possible rules by requiring balance, first-order correlation immunity, nonlinearity, and the Strict Avalanche Criterion, leaving 7,080 candidates. These are tested as pseudo-random generators using NIST FIPS 140-2; 53 rules pass. Enforcing bijectivity leaves a single valid rule, whose ANF is

$$x_0x_3 + x_1x_3 + x_2x_3 + x_3x_4 + x_1 + x_2 + x_3 + 1.$$

Results.

Property	**Our 10-bit S-Box**	**AES S-Box**	**Comparison**
Min/Max algebraic degree	8-9	7-7	Better
Algebraic complexity	1023	255	Equivalent
Nonlinearity	434 (=108.5*4)	112	Worse
Strict Avalanche Criterion	0.44-0.5-0.57	0.45-0.5-0.56	Worse
Bit Independence Criterion	0.124	0.134	Better
Lin. Approx. Probability	9.28%	6.25%	Worse
Diff. Approx. Probability	1.37%	1.56%	Better
Differential Uniformity	14	4	Worse
Boomerang Uniformity	24	6	Worse

Figure 3: Comparison of the security properties of our 10-bit S-Box and the 8-bit S-Box from AES (normalized results).

The code we used to generate our 10-bit S-Box is available at https://github.com/thomasarmel/luby_rackoff_sbox_finder .

References:

1. Feistel, H.: Cryptography and computer privacy. Scientific american (1973)
2. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing (1988).
3. Wolfram, S.: Statistical mechanics of cellular automata. Reviews of modern physics (1983).

Ключові слова: блоковий шифр на основі S-блоків, клітинні автомати, мережа Фейстеля, булеві функції.
Keywords: S-box Block cipher, Cellular automata, Feistel permutation, Boolean functions.

СИСТЕМИ РАНЖУВАННЯ ТА АНАЛІЗУ ІНФОРМАЦІЇ ПРИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Кухаренко Сергій

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Сидорчук Владислав

Національний університет «Одеська юридична академія», PhD в галузі права, доцент кафедри кримінального процесу

Стрімке зростання кількості кіберінцидентів потребує створення ефективних систем їх обробки та аналізу. За даними CERT-UA, у 2024 році було опрацьовано 4315 кіберінцидентів, що на 69,8% більше порівняно з 2023 роком [1]. Це актуалізує необхідність впровадження автоматизованих систем ранжування та інтелектуального аналізу даних для оптимізації протидії кіберзлочинам.

Метою дослідження є розробка практичної системи ранжування інформації про кіберінциденти та визначення ключових напрямків аналізу даних для ефективної протидії кіберзлочинам.

1. Методи збору інформації про кіберінциденти

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки в Україні", кіберінцидент визначається як подія або ряд несприятливих подій, які становлять загрозу безпеці електронних комунікаційних систем та створюють імовірність порушення їх штатного режиму
функціонування [2].

Для ефективного збору інформації про кіберінциденти застосовуються різноманітні методи та технології:

1.1. Системи виявлення та запобігання вторгненням (IDS/IPS) здійснюють моніторинг мережевого трафіку в режимі реального часу, виявляючи підозрілу активність. До таких систем належать Snort, Suricata, Zeek та Cisco Firepower [3]. Основною перевагою є автоматичне блокування атак, проте вони характеризуються високим рівнем помилкових спрацювань.

1.2. SIEM-системи (Security Information and Event Management) забезпечують централізований збір, аналіз і кореляцію логів з різних джерел. Популярні рішення включають Splunk, IBM QRadar, ArcSight та Elastic Stack [4]. Це потужний інструмент аналітики, але характеризується високою вартістю та складністю впровадження.

1.3. Threat Intelligence платформи спеціалізуються на зборі, аналізі та обміні даними про загрози. Використання таких платформ як MISP,

ThreatConnect, Anomali забезпечує проактивний захист та контекстуалізацію загроз [5].

1.4. DLP системи (Data Loss Prevention) запобігають витоку конфіденційних даних, контролюючи їх передачу. Рішення від Symantec, McAfee та Forcepoint DLP забезпечують compliance, але можуть обмежувати робочі процеси [6].

1.5. Honeypots/Honeynets – системи-приманки для залучення атакуючих, що дозволяють вивчати їх тактики та отримувати раннє попередження про загрози [7].

В Україні функціонує національна система реагування на кіберінциденти, ключовим елементом якої є CERT-UA. Цей орган здійснює моніторинг, накопичення та проведення аналізу даних про кіберінциденти на національному рівні [2]. Згідно з Порядком взаємодії суб'єктів національної системи реагування, CERT-UA невідкладно інформує СБУ про значні кіберінциденти щодо об'єктів критичної інфраструктури та Національну поліцію – про кібератаки на такі об'єкти [8].

2. Система ранжування кіберінцидентів

Зважаючи на постійне зростання кількості кіберінцидентів, критично важливою є розробка системи їх ранжування для визначення пріоритетності реагування (дивись рисунок 1).

Рисунок 1 – Алгоритм ранжування кіберінциндентів

2.1. Критерії ранжування

Запропонована система базується на шести ключових критеріях:

1. Об'єкт інциденту:
– об'єкт критичної інфраструктури або військовий об'єкт – 3 бали;
– державна або комунальна установа – 2 бали;
– приватна установа – 1 бал.
2. Ризики для обороноздатності держави:
– катастрофічні наслідки – 3 бали;
– значні наслідки – 2 бали;
– незначні наслідки – 1 бал;
– відсутні наслідки – 0 балів.
3. Розмір матеріального збитку:
– катастрофічний збиток – 3 бали;
– значний збиток – 2 бали;
– незначний збиток – 1 бал;
– відсутній збиток – 0 балів.
4. Джерело інциденту:
– зовнішнє джерело – 2 бали;
– внутрішнє джерело – 1 бал.
5. Рівень складності атаки:
– складна, багатоетапна атака – 3 бали;
– середній рівень складності – 2 бали;
– низький рівень складності – 1 бал;
– відсутні ознаки кібератаки – 0 балів.
6. Статус активності:
– активна загроза – 3 бали;
– неактивна загроза – 0 балів.

2.2. Формула розрахунку рангу.

Для визначення рангу кіберінциденту використовується формула:

$R = \Sigma(O)$

де O – оцінка за кожним критерієм.

Діапазон можливих значень: $2 \leq R \leq 17$

2.3. Класифікація за рівнями небезпеки

– Високий рівень небезпеки: 11-17 балів
– Середній рівень небезпеки: 5-10 балів
– Низький рівень небезпеки: 2-4 бали

Така система дозволяє автоматизувати процес пріоритизації реагування на інциденти та оптимізувати розподіл ресурсів служб кібербезпеки.

3. Напрямки аналізу даних за допомогою data mining

Data Mining – процес автоматичного виявлення прихованих закономірностей у необроблених даних, які мають практичну цінність та можуть бути інтерпретовані людиною [9]. При протидії кіберзлочинам технології Data Mining застосовуються у наступних напрямках:

3.1. Аналіз мережевого трафіку

Спрямований на виявлення несанкціонованого доступу (спроби підключення до закритих портів, експлуатація вразливостей), зловмисного програмного забезпечення (поширення вірусів, шифрування файлів) та витоку даних (несанкціонована передача конфіденційної інформації). Додатково здійснюється контроль дотримання політики безпеки.

3.2. Аналіз поведінки користувачів

Дозволяє виявляти аномальну активність користувачів, внутрішні загрози (співробітники, які викрадають дані або обходять політику безпеки) та будувати поведінкові профіли, що включають середній час активності, типи використовуваних файлів, характер мережевого трафіку та частоту авторизацій.

3.3. Аналіз фішингу

Застосовується для автоматичного виявлення фішингових листів через аналіз структури тексту, наявності підозрілих посилань та маніпулятивного стилю. Включає аналіз URL-адрес та доменів, виявлення фішингових доменів за схожістю до легітимних, знаходження новостворених доменів та аналіз підозрілих редиректів.

3.4. Аналіз вразливостей

Поділяється на два напрямки:

Аналіз «вразливостей» осіб: визначення категорій користувачів, схильних до ризикованої поведінки (відкриття небезпечних листів, відвідування підозрілих сайтів, використання слабких паролів). Формування індивідуальних профілів ризику дозволяє запобігти інсайдерським загрозам.

Аналіз технічних вразливостей: виявлення програмних вразливостей у системах, мережевих аномалій, слабкостей автентифікації, конфігураційних помилок та вразливостей у хмарних сховищах.

3.5. Кластеризація кіберзагроз та інцидентів

Дозволяє групувати однотипні атаки, виявляти приховані закономірності між інцидентами, будувати таксономію загроз, здійснювати пріоритизацію реагування та виявляти нові типи атак.

3.6. Асоціативний аналіз подій

Встановлює причинно-наслідкові зв’язки між подіями, виявляє залежності між кроками атаки, створює асоціативні правила типу "якщо-то", формує індикатори безпеки та автоматизує реагування на інциденти.

Висновки

1. Протидія кіберзлочинам потребує комплексного підходу, що включає використання різноманітних методів збору інформації про кіберінциденти – від систем IDS/IPS до SIEM-систем та Threat Intelligence платформ.

2. Розроблена система ранжування кіберінцидентів на основі шести критеріїв дозволяє автоматизувати процес визначення пріоритетності реагування та ефективно розподіляти ресурси служб кібербезпеки.

3. Застосування технологій Data Mining у протидії кіберзлочинам відкриває можливості для глибинного аналізу мережевого трафіку, поведінки користувачів, виявлення фішингу, аналізу вразливостей та кластеризації загроз.

4. Інтеграція систем ранжування з методами інтелектуального аналізу даних створює потужний інструментарій для проактивного запобігання кіберзлочинам та оперативного реагування на кіберінциденти.

5. Подальший розвиток систем протидії кіберзлочинам має включати впровадження технологій штучного інтелекту з обов'язковим контролем якості результатів та врахуванням потенційних ризиків автоматизованого прийняття рішень.

Список використаних джерел:

1. CERT-UA минулого року опрацювала 4315 кіберінцидентів. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
2. Про основні засади забезпечення кібербезпеки в Україні : Закон України від 05 жовтня 2017 року, № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Що таке (IPS/IDS) і де застосовується. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujet-sya
4. Смірнова Т., Константинова Л., Конопліцька-Слободенюк О., Козлов Я., Кравчук О., Козірова Н., Смірнов О. Дослідження сучасного стану SIEM-систем. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2024. № 1(25). С. 6–18. https://doi.org/10.28925/2663-4023.2024.25.618
5. Дорохін О.О., Марченко В.В., Семенова І.Д. Технологія threat intelligence та методи її використання для захисту компанії від кіберзагроз. Сучасний захист інформації. 2021. № 3(47). С. 12-16.
6. Гайдур Г., Марченко В., Борсуковський Ю., Дмітрієв В., Царьова С. DLP-система як компонент протидії інсайдерським загрозам конфіденційності інформації. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. № 2(30). С. 583–592. https://doi.org/10.28925/2663-4023.2025.30.995
7. Притула А. В., Куперштейн Л. М. Технологія honeypot як альтенативний підхід виявлення вразливостей. Вінницький національний технічний університет, Вінниця. URL: https://surl.li/fujlqo

8. Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності : Постанова КМУ від 13 листопада 2025 року, № 1471. URL: https://zakon.rada.gov.ua/laws/show/1471-2025-п#n8
9. DataMining з використанням Python. Навчальний посібник // Юрченко І.В.– Чернівці: Чернівецький національний університет імені Юрія Федьковича, 2024.– 143 с. URL: https://surl.lu/szhxwy

Ключові слова: кібербезпека, управління кібербезпекою, кіберінцидент, кіберзлочин, ранжування кіберінциндентів, методи та засоби кібербезпеки.
Key words: cybersecurity, cybersecurity management, cyber incident, cyber crime, cyber incident ranking, cybersecurity methods and tools

БЕЗПЕКА ANDROID-ЗАСТОСУНКІВ НА KOTLIN ТА JETPACK COMPOSE

Манаков Сергій
кандидат технічних наук, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Безпека мобільних застосунків у 2025 році стає актуальною компетенцією для розробників через швидку еволюцію загроз. Нативні Android-застосунки на Kotlin та Jetpack Compose вимагають особливого підходу до безпеки. Метадані компілятора Kotlin зберігають оригінальні імена навіть після обфускації, що спрощує зворотну розробку [1]. Дослідження показують, що жорстко закодовані API-ключі легко витягуються з APK, а багато застосунків використовують SharedPreferences без шифрування.

Основні загрози включають неправильне поводження з обліковими даними, слабку автентифікацію, недостатній захист бінарних файлів та небезпечне зберігання даних [2]. Особливої актуальності набула безпека ланцюга постачання для Compose-застосунків через інтенсивне використання залежностей та відсутність специфікації Software Bill of Materials. Важливою зміною 2025 року стала депрекація бібліотеки androidx.security:security-crypto, що вимагає міграції на пряме використання Android Keystore (база даних сертифікатів безпеки, яка створюється за допомогою програми keytool із пакету SDK для Java).

Практичні дослідження виявляють систематичні помилки безпеки в Kotlin-застосунках [3]. Серед найпоширеніших – жорстко закодовані облікові дані, зберігання секретів у налаштуваннях збирача проєктів gradle, ігнорування обфускації метаданих Kotlin та відсутність обробника винятків корутин CoroutineExceptionHandler. Специфічними для Compose помилками є зберігання чутливих даних у remember, витоки пам'яті через неправильне

використання DisposableEffect та захоплення у лямбда-виразах, що утримуються у ViewModel.

Для захисту даних Android Keystore System забезпечує апаратну ізоляцію ключів [4]. Рекомендованими алгоритмами є AES-256-GCM, ChaCha20-Poly1305 та ECC P-256+. Заборонено використовувати DES, 3DES, RC4, MD5, SHA-1 та RSA з ключами менше 2048 біт [5]. Для захисту локального сховища слід використовувати Encrypted Room з SQLCipher, а для DataStore реалізовувати власний шар шифрування. Ієрархія безпеки для зберігання ключів включає проксі на стороні сервера, Android Keystore, сховище NDK/C++ та BuildConfig.

Безпека API вимагає комплексного підходу [6]. У Retrofit та OkHttp захист забезпечується через interceptor'и та authenticatori', які автоматично обробляють оновлення токенів. Ktor Client має вбудовану підтримку плагіну Auth з механізмом оновлення та захистом від атак DoS. Google не рекомендує закріплення сертифіката (certificate pinning), але якщо таке необхідне, слід використовувати резервні сертифікати (backup pins) та моніторинг терміну дії [7]. Network Security Configuration є рекомендованим методом 2025 року для налаштування безпеки мережі. Для автентифікації слід використовувати OAuth 2.0 та JWT, при цьому PKCE є обов'язковим для нативних застосунків. Найкращі практики для JWT включають короткий термін дії, валідацію при кожному використанні, зберігання в EncryptedSharedPreferences та використання м'ютекса для оновлення токена.

Специфіка безпеки Jetpack Compose включає проблему з наслідуванням FLAG_SECURE у спливаючих вікнах, що призводить до витоку даних через знімки екрана. Також, використання immutable String для полів паролів унеможливлює їх очищення з пам'яті, дозволяючи вилучення через дампи пам'яті. В свою чергу, поширеною проблемою є витоки даних через керування станом, коли remember зберігає чутливі дані довше, ніж потрібно, а також витоки пам'яті через захоплення у лямбда-виразах та неправильне використання DisposableEffect.

Інтеграція DevSecOps також стає необхідністю [8]. Підхід Shift-left security передбачає інтеграцію перевірок безпеки з першого дня розробки. Для статичного та динамічного аналізу використовуються інструменти MobSF, Detekt та SonarQube [9]. Безпековий конвеєр в GitHub Actions може включати валідацію Gradle Wrapper, Detekt, сканування через MobSF та OWASP Dependency-Check. Шлюзи безпеки (security gates) в CI/CD блокують збірки з критичними вразливостями. Для тестування на проникнення застосовують Frida, Objection, Drozer та Burp Suite [10].

Практичні рекомендації включають використання Android Keystore для ключів, EncryptedSharedPreferences для токенів, вимкнення логування чутливих даних та резервних копій (android:allowBackup=false), використання

FLAG_SECURE. Для криптографії слід застосовувати AES-256-GCM та SecureRandom. В автентифікації рекомендовані Credential Manager API, Passkeys, біометрія, валідація JWT та механізми захисту від перебору. Мережева безпека вимагає TLS 1.2+ та відмови від нешифрованого трафіку (cleartextTrafficPermitted=false). Безпека платформи передбачає мінімальні дозволи та валідацію вхідних даних. Якість коду забезпечується обфускацією ProGuard/R8, регулярним оновленням залежностей та використанням Play Integrity API.

Отже, безпека Android-застосунків на Kotlin та Jetpack Compose у 2025 році вимагає комплексного підходу. Обфускація є недостатньою через розкриття метаданих Kotlin. Депрекація бібліотеки Jetpack Security crypto вимагає глибокого розуміння Android Keystore API. Jetpack Compose створює виклики, пов'язані з FLAG_SECURE, обробкою паролів та витоками пам'яті. Інтеграція інструментів DevSecOps (MobSF, Detekt) в CI/CD стала необхідністю. Підхід Shift-left security забезпечує раннє виявлення вразливостей, що суттєво знижує вартість виправлення. Основні рекомендації розробникам являють: використання Android Keystore, імплементація OAuth 2.0 з PKCE, обережне застосування закріплення сертифіката, регулярне оновлення залежностей та проведення тестування безпеки.

Список використаних джерел

1. Mazuera-Rozo A., Escobar-Velásquez C., Espitia-Acero J., Vega-Guzmán D., Trubiani C., Linares-Vásquez M., Bavota G. Taxonomy of security weaknesses in Java and Kotlin Android apps. *Journal of Systems and Software*. 2022. Vol. 187. P. 111233. DOI: https://doi.org/10.1016/j.jss.2022.111233
2. Garg S., Baliyan N. Android security assessment: A review, taxonomy and research gap study. *Computers & Security*. 2021. Vol. 100. P. 102087. DOI: https://doi.org/10.1016/j.cose.2020.102087
3. Egele M., Brumley D., Fratantonio Y., Kruegel C. An empirical study of cryptographic misuse in android applications. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013. P. 73-84. DOI: https://doi.org/10.1145/2508859.2516693
4. Enck W., Nadkarni A. Android's Security Framework: Understanding the Security of Mobile Phone Platforms. Encyclopedia of Cryptography, Security and Privacy. Springer, 2021. DOI: https://doi.org/10.1007/978-3-642-27739-9_121-2
5. Kalanj M., Popović T., Krčo S. Analysis of Cryptography Algorithms Implemented in Android Mobile Application. *Information Technology and Control*. 2021. Vol. 50, No. 4. P. 786-803. DOI: https://doi.org/10.5755/j01.itc.50.4.29464
6. Sun Y., Wang Y., Zhang Q., Chen K. CryptoEval: Evaluating the risk of cryptographic misuses in Android apps with data-flow analysis. *IET Information Security*. 2023. Vol. 17, No. 4. P. 564-580. DOI: https://doi.org/10.1049/ise2.12117
7. Ardito L., Coppola R., Malnati G., Torchiano M. Effectiveness of Kotlin vs. Java in android app development tasks. *Information and Software Technology*. 2020. Vol. 127. 106374. DOI: https://doi.org/10.1016/j.infsof.2020.106374

8. Abiona O. O., Oladapo O. J., Modupe O. T., Oyeniran O. C., Adewusi A. O., Komolafe A. M. The emergence and importance of DevSecOps: Integrating and reviewing security practices within the DevOps pipeline. *World Journal of Advanced Engineering Technology and Sciences*. 2024. Vol. 11, No. 2. P. 127-133. DOI: https://doi.org/10.30574/wjaets.2024.11.2.0093
9. Zhao X., Hoda R., Clear T., MacDonell S. G. Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. *Journal of Systems and Software*. 2024. Vol. 214. 112059. DOI: https://doi.org/10.1016/j.jss.2024.112059
10. Akbar M. A., Smolander K., Mahmood S., Alsanad A. Toward successful DevSecOps in software development organizations: A decision-making framework. *Information and Software Technology*. 2022. Vol. 147. 106894. DOI: https://doi.org/10.1016/j.infsof.2022.106894

Ключові слова: безпека Android, Kotlin, Jetpack Compose, криптографія мобільних застосунків, DevSecOps, вразливості застосунків, захист даних.
Keywords: Android security, Kotlin, Jetpack Compose, mobile application cryptography, DevSecOps, application vulnerabilities, data protection.

КОНЦЕПЦІЯ ТА РОЗГОРТАННЯ ВИСОКОІНТЕРАКТИВНОГО ХАНІПОТУ НА НА ОСНОВІ ЕМУЛЯЦІЇ ЛЕГІТИМНОГО ВЕБСЕРВЕРА (NGINX)

Бойко Віктор
кандидат технічних наук, доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Ханіпотом (медовим горщиком) називають спеціальний пасивний засіб захисту — по суті, пастку, що є приманкою для шкідливого програмного забезпечення. По суті, це — спеціалізований пасивний засіб збору розвідувальних даних, що є приманкою для зловмисників та шкідливого ПЗ, основне завдання якого виявляти нові й цільові атаки Zero-day, які погано піддаються розпізнаванню традиційними методами [1].

Існуючі рішення для ханіпотів традиційно поділяються на дві основні категорії: низькоінтерактивні та високоінтерактивні. Низькоінтерактивні ханіпоти, як-от Cowrie (для емуляції SSH) або Dionaea (для мережевих сервісів), швидко емулюють лише необхідні аспекти реального сервісу, що робить їх економічними, але водночас вкрай вразливими до автоматизованого розпізнавання досвідченими ботами та зловмисниками. Натомість, високоінтерактивні ханіпоти використовують повну віртуалізацію операційної системи або сервісу, що вимагає значно більших ресурсів, але надає максимально детальні та цінні розвідувальні дані про поведінку атакуючого. Більшість готових комерційних та open-source рішень часто є гібридами, які намагаються знайти баланс між ресурсоємністю та глибиною взаємодії, проте їхня широка відомість і типові мережеві відбитки є головною вразливістю [2].

Сучасне шкідливе програмне забезпечення (malware) характеризується, з одного боку, постійним удосконаленням методів атаки та еволюцією засобів нападу, з іншого — високим рівнем використання автоматичних, практично “бездумних” засобів атаки [3].

Ботнети являють собою децентралізовані мережі, які складаються з мільйонів скомпрометованих пристроїв, включаючи традиційні сервери, робочі станції, а також пристрої Інтернету речей (IoT), що мають мінімальний рівень захисту. Саме широке використання IoT як вектора атаки стало ключовим фактором зростання ботнет-активності (зафіксовано зростання на 25% у 2023 році). Ботнети, такі як Torpig Mebroot або TorrentLocker, забезпечують зловмисників масштабованою платформою для розповсюдження шкідливого ПЗ, спаму та проведення DDoS-атак. Крім того, такі угруповання, як Volt Typhoon, використовують ботнети для прихованого проникнення та закріплення в мережах критичної інфраструктури, що вимагає вкрай складних методів виявлення, які не здатні забезпечити традиційні сигнатурні засоби[4].

Широке використання систем LLM призвело до того, що боти, з одного боку, швидко вдосконалюються та змінюються. З іншого боку, використання LLM значною мірою стандартизує та “шаблонізує” техніки, що використовуються ботами. У звіті [5] вказується вплив усіх перелічених вище факторів. Автоматизований трафік перевищив людський: Вперше автоматизований трафік (боти) становив 51% від усього інтернет-трафіку, перевищивши людський (49%). При цьому шкідливі боти (які часто є частиною ботнетів) зросли до 37% від усього веб-трафіку (це шостий рік поспіль зростання). Автори звіту роблять висновок про те, що доступність інструментів ШІ сприяла зростанню простих бот-атак (вони зросли до 45% усіх бот-атак), оскільки ШІ знизив поріг входу для зловмисників. Вплив ШІ двоякий: зростання простих, шаблонізованих атак (45% бот-трафіку, за Imperva) збільшує загальний шум, але ШІ також дозволяє ботам будь-якого класу швидше адаптуватися та мімікрувати, що робить їх більш ухильними (advanced evasion) від традиційних засобів захисту. Такий стан справ вимагає використання нетрадиційних засобів, що доповнюють традиційні (IDS/IPS/Firewalls).

Швидка еволюція та простота арсеналу сторони, що атакує, вимагає такого ж швидкого виявлення та аналізу атак. Це висуває ханіпоти, як систему, що дозволяє швидко зібрати інформацію та виявити можливі методи атаки, на перший план. Однією з проблем пропонованих готових рішень є їхня широка відомість — зокрема зловмисникам, що дозволяє вибудовувати системи протидії таким пасткам.

Пропонована система використовує як фронтенд вебсервер Nginx. Така схема дозволяє отримати одразу кілька переваг. Перше — це суттєва економія ресурсів як у процесі розробки ханіпоту (не потрібно створювати

блок, що відповідає за взаємодію з вебпротоколами), так і в процесі експлуатації (Nginx розрахований на максимізацію продуктивності та добре справляється там, де потрібне кешування), друге — використання реального вебсервера з усіма його властивостями та ознаками дозволяє замаскувати цільове призначення медової пастки та ввести атакуючого в оману. Використання реального, надійно сконфігурованого вебсервера дозволяє точно імітувати мережевий відбиток (network fingerprint) легітимної системи. Nginx генерує реалістичні заголовки відповідей (HTTP response headers) та обробляє мережеві запити з очікуваною швидкістю та поведінкою, що значно ускладнює автоматизоване виявлення пастки на основі відомих сигнатур, які використовують досвідчені зловмисники.

Системи, що використовують цю ідею в пілотному варіанті, були розгорнуті 27 липня 2025 року. На 01 листопада 2025 року було зібрано 136615 записів. Цікавим побічним ефектом експлуатації системи стала можливість проспостерігати в режимі реального часу зростання активності ботнетів, пов'язане з кількома великими DDoS-атаками: атаку на Cloudflare 2-го вересня [6], та атаку на сервери MMORPG Albion Online (офіційний звіт на форумі компанії [7]) 23 липня (рис.1).

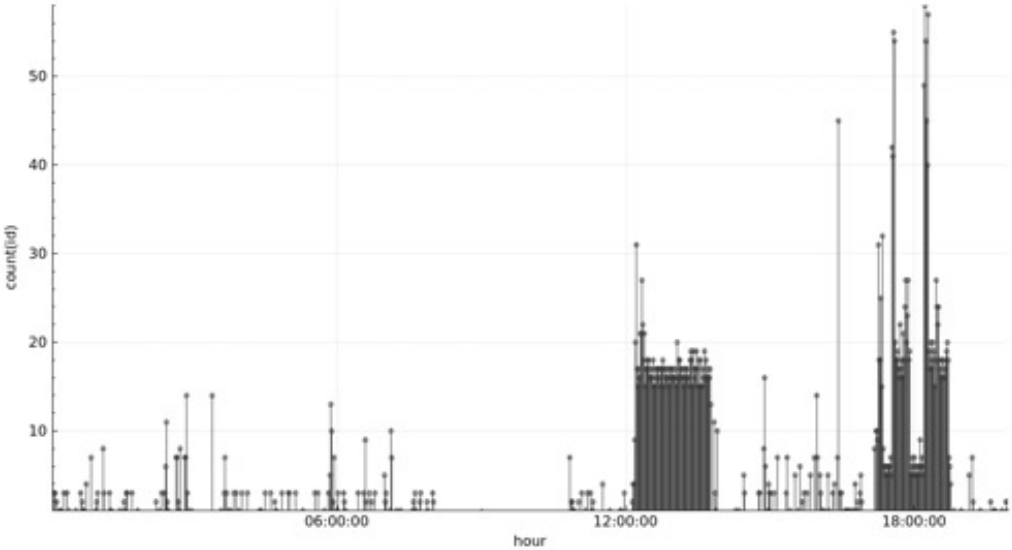

Рисунок 1 – Кількість атак 23-го липня 2025 року

Надалі така інформація може бути використана для прогнозування нових DDoS-атак, оскільки їхній початок, можливо, пов'язаний зі зростанням загальної активності ботнету, яку може виявляти пропонований ханіпот.

Список використаних джерел:

1. *Morić Z., Dakić V., Regvart D.* Advancing Cybersecurity with Honeypots and Deception Strategies // Informatics. MDPI, 2025. T. 12. 14.
2. *Zou J., Sun Z., Ku C., Li X., Dahbura A.* WiP: Developing High-interaction Honeypots to Capture and Analyze Region-Specific Bot Behaviors // Proceedings of the Hot Topics in Security and Privacy (HotSoS). JHU Information Security Institute, 2024.

3. *Insikt Group, Recorded Future*. 2024 Malicious Infrastructure Report: Threat Intelligence Report. — Recorded Future, 2025.
4. *USTelecom*. Botnet and IoT Security Trends 2024: Industry Report. — USTelecom, 2024. — URL: https://ustelecom.org/wp-content/uploads/2024/03/USTelecom-Botnet-and-Security-Trends-2024.pdf.
5. *Imperva Threat Research, Thales*. 2025 Bad Bot Report: The Rapid Rise of Bots and The Unseen Risk for Business: Annual Report. — Imperva, 2025. — URL: https://www.imperva.com/resources/resource-library/reports/2025-bad-bot-report/.
6. *SecurityOnline Info*. The Largest DDoS Attack in History: Cloudflare Fights Back. — https://securityonline.info/the-largest-ddos-attack-in-history-cloudflare-fights-back/, 2025.
7. *Sandbox Interactive, Albion Online Forum*. Resolved: Ongoing DDoS Attack & Compensation (Forum Post). — https://forum.albiononline.com/index.php/Thread/214699-Resolved-Ongoing-DDoS-Attack-Compensation/#post1442554, 2025.

Ключові слова: ханіпот, високоінтерактивний, nginx, ботнет, виявлення атак, zero-day, мережевий відбиток, емуляція, кібербезпека, автоматизований трафік, вебсервер, розвідувальні дані, ddos-атака, маскування, шкідливе пз, віртуалізація, журналювання, мережева інфраструктура, критична інфраструктура, сигнатури.
Keywords: honeypot, high-interaction, nginx, botnet, attack detection, zero-day, network fingerprint, emulation, cybersecurity, automated traffic, web server, threat intelligence, ddos attack, deception, malware, virtualization, logging, network infrastructure, critical infrastructure, signatures

МІЖНАБОРНЕ ТЕСТУВАННЯ МЕТОДУ KNN+TF-IDF У ЗАДАЧІ ВИЯВЛЕННЯ ІН'ЄКЦІЙНИХ АТАК У ВЕБ-ЗАПИТАХ

Коробейнікова Тетяна

к.т.н., доцент, доцент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка»

Кравчук Назар

аспірант, асистент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка»

У сучасних вебзастосунках, що характеризуються великою кількістю динамічних інтеграцій і складною структурою даних, ризик появи ін'єкційних атак (SQLi, XSS, ін'єкцій команд) залишається одним із ключових викликів для систем кіберзахисту. Традиційні сигнатурні рішення IDS/WAF часто не здатні ефективно розпізнавати обфусковані або нові варіанти атак, тоді як моделі глибинного навчання вимагають значних обчислювальних ресурсів і не завжди забезпечують прозорість прийняття рішень. У попередній роботі нами було показано, що поєднання алгоритму k-найближчих сусідів (KNN) із TF-IDF-представленням текстових навантажень і додатковими структурно-статистичними ознаками дозволяє досягти високої ефективності виявлення ін'єкцій (до 99,77% точності та F_1=0,998) при низьких ресурсних витратах.

У цьому дослідженні ми зосередили увагу на міжнаборному тестуванні (Cross-Dataset Evaluation) для оцінювання узагальнювальної здатності вдосконаленої моделі KNN+TF-IDF. Головною метою є перевірка стійкості моделі до зміни домену даних — тобто її здатності коректно класифікувати ін'єкційні атаки з наборів даних, що не використовувалися під час навчання.

Експериментальне оцінювання проводилося на трьох відкритих наборах даних: HttpParamsDataset (навчальний корпус), SQLi/XSS Dataset та OS Command Injection Dataset. Для базової моделі використовувалася лише TF-IDF-векторизація тексту, тоді як вдосконалена модель включала сім додаткових числових ознак: довжину навантаження, кількість цифр, кількість великих літер, щільність спеціальних символів, ентропію, індикатор логічних тавтологій і сигнатури системних команд.

Таблиця 1 подає порівняльні результати базової та вдосконаленої моделей на невідомих наборах даних. Як і очікувалося, точність знижується, коли моделі, навчені на HttpParamsDataset, стикаються з новими структурами навантажень. Однак розширений набір ознак суттєво пом'якшує це погіршення, забезпечуючи покращення як точності Accuracy, так і зваженого показника $F_{1\text{-weighted}}$.

Таблиця 1 - Результати узагальнення між наборами даних (Cross-Dataset Generalization Results)

Dataset	k	Metric	Accuracy	$F_{1-weighted}$
SQLi/XSS (Baseline)	5	Cosine	0.6475	0.6431
SQLi/XSS (Improved)	5	Cosine	0.7674	0.7688
Command Injection (Baseline)	5	Cosine	0.8527	0.8305
Command Injection (Improved)	5	Cosine	0.8741	0.8533

Список літератури

1. Таченко І. А. Огляд сучасного стану питання в галузі оцінювання ризиків мережевої безпеки / І. А. Таченко, Т. І. Коробейнікова, С. М. Захарченко // Scientific Collection «InterConf», (84): with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021). Rome, Italy: Dana, 2021. 478 p. – С. 417-432.
2. ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management. International Organization for Standardization.
3. NIST SP 800-37 Rev. 2. (2018). Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. National Institute of Standards and Technology.
4. ENISA. (2020–2024). Threat Landscape Reports. European Union Agency for Cybersecurity.

Ключові слова: ін'єкційні атаки, виявлення атак, KNN, TF-IDF.
Keywords: injection attacks, attack detection, KNN, TF-IDF.

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ СУЧАСНОГО РИНКУ ВІДЕОІГОР

Куклінова Тетяна

кандидат економічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Гулієва Анастасія

студентка 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету«Одеська юридична академія»

Сучасний ринок відеоігор є одним із найдинамічніших сегментів цифрової економіки. За останні десять років відеоігри перетворилися з розважального хобі на глобальний технологічний феномен, який поєднує індустрію розваг, цифрові сервіси, штучний інтелект, соціальні мережі та елементи віртуальної економіки. Так, ігрова індустрія сьогодні налічує сотні мільйонів гравців по всьому світу і є ключовим драйвером розвитку цифрового контенту, нових форм віртуальної взаємодії та економічного зростання. Вона охоплює не лише комп'ютерні та мобільні ігри, а й онлайн-платформи, кіберспорт, віртуальні світи та хмарні технології, про що свідчить Рис.1.

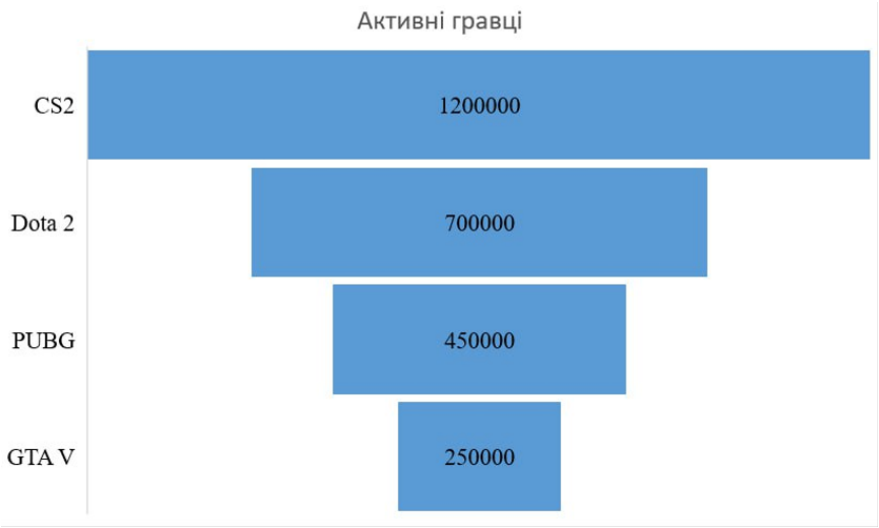

Рис. 1. Кількість активних гравців популярних ігор (Steam) станом на 01.01.2025 [1]

Зазначимо, що однією з провідних тенденцій розвитку індустрії є поширення хмарного геймінгу та стрімінгових сервісів, що дозволяють запускати ігри без потреби у потужному обладнанні, а традиційна модель володіння іграми поступово замінюється підпискою на доступ до великої бібліотеки контенту. Паралельно зростає використання штучного інтелекту для створення реалістичної поведінки персонажів та персоналізації ігрового досвіду. Розробники активно інтегрують технології доповненої та віртуальної реальності, розвивають жанр соціальних онлайн-ігор, де формується спільний простір для взаємодії мільйонів користувачів.

Також важливим напрямом трансформації ринку є формування внутрішньої цифрової економіки відеоігор. Її основою стали мікротранзакції, внутрішньоігрові покупки та використання віртуальних валют. У деяких іграх створюються повноцінні економічні системи, де гравці купують або продають предмети, персонажів чи акаунти. Цей процес посилюється із розвитком блокчейн-технологій, що дозволяють створювати та передавати унікальні цифрові об'єкти з доказом власності. Проте такий напрям потребує регулювання, оскільки межує з реальними фінансовими операціями та може спричиняти кіберзлочинність.

Але популярні мережеві ігри також стають основною ціллю кіберзлочинців. Так, у грі Counter-Strike 2 щотижня фіксуються масові випадки викрадення акаунтів через фішингові сайти, що імітують Steam Login. Також поширене шахрайство зі скінами, які мають реальну ринкову вартість, перетворює гру на інструмент тіньового обміну цифрових активів. Аналогічна ситуація спостерігається в Dota 2, де кіберзловмисники використовують бот-мережі для викрадення акаунтів із високим рейтингом MMR та поширюють шкідливе програмне забезпечення під виглядом скриптів. Популярним методом атак залишається соціальна інженерія, коли шахраї виманюють дані входу, обіцяючи «прокачування персонажа» або вигідний обмін [1] (Рис.2).

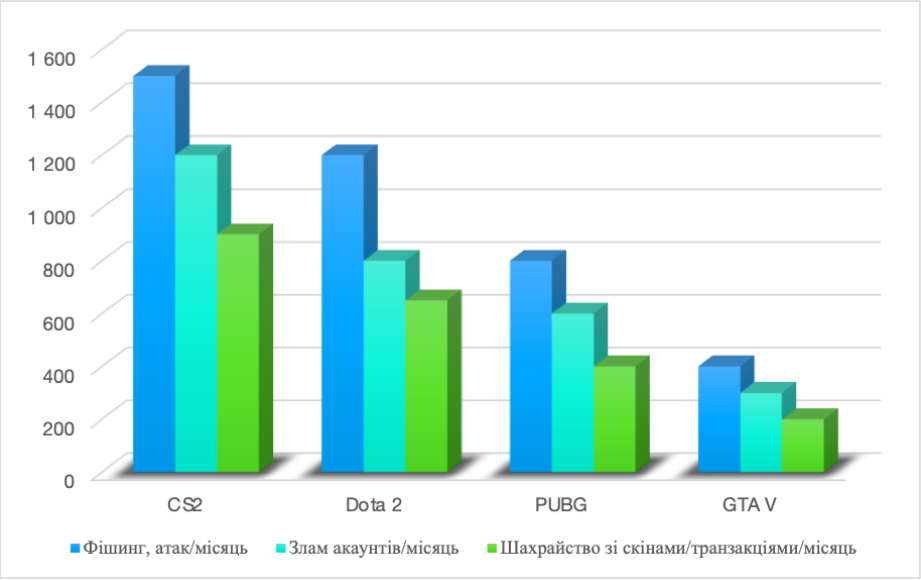

Рис. 2 Статистика кіберзагроз у популярних іграх Steam у 2024рр.[1]

Швидке зростання галузі супроводжується значним збільшенням кіберзагроз. Щодня здійснюються тисячі зламів облікових записів, викрадень даних користувачів, фінансових махінацій та хакерських атак на ігрові сервери. Масового характеру набули атаки типу DDoS, які призводять до відмови серверів у роботі [2]. Злочинці використовують автоматизовані інструменти для підбору паролів, що дозволяє захоплювати акаунти, які часто пов'язані з банківськими картками або іншими платіжними даними [3].

Особливої уваги потребує захист неповнолітніх користувачів. Велика частина аудиторії відеоігор – підлітки та молодь, що робить їх вразливими до маніпуляцій, онлайн-булінгу, грумінгу та шахрайства.

Серйозною загрозою є також розповсюдження шкідливого програмного забезпечення під виглядом модів, читів або безкоштовних доповнень. Після встановлення такі програми виявляються вірусами, що викрадають персональні дані або надають хакеру дистанційний доступ до комп'ютера користувача. Уразливості можуть міститися навіть в офіційних ігрових клієнтах через недосконале тестування безпеки, особливо у багатокористувацьких іграх із великим мережевим навантаженням.

Підкреслюється, що, особлива увага має бути приділена аспектам кібербезпеки, які є критично важливими для захисту персональних даних користувачів та цілісності платформи Необхідно передбачити інтеграцію систем захисту, регулярне тестування на вразливості та оперативне реагування на інци-денти. Окрім технічних засобів, слід впроваджувати політики інформаційної безпеки для користувачів і персоналу. [4].

Отже, розв'язання проблем кібербезпеки вимагає комплексного підходу: застосування багатофакторної автентифікації, регулярні оновлення програмного забезпечення, захист серверів від DDoS-атак, моніторинг підозрілої активності, а також навчання користувачів основам кібергігієни. Ігрові компанії повинні впроваджувати принцип «безпека за задумом», передбачаючи проєктування систем з урахуванням захисту з самого початку розробки. Водночас її розвиток супроводжується зростанням кіберзагроз, що створює ризики для мільйонів користувачів і компаній. Подальший поступ ринку можливий лише за умови поєднання технологічних інновацій із підвищеною увагою до кібербезпеки, етичних стандартів обробки даних та міжнародної співпраці у сфері цифрового захисту.

Список використанних джерел:

1. SteamDB. Counter-Strike 2. URL: https://steamdb.info/app/730/
2. Imperva. Comprehensive digital security. URL: https://www.imperva.com/blog/understanding-cyber-threats-in-gaming/?utm_source
3. Cloudflare. DDoS-огляди та аналітика. URL: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/?utm_source=chatgpt.com/
4. Куклінова Т.В., Чепурна О.Є., Куклінова С.І. Проєктне управління розробкою веб порталу для цифрових спільнот геймерів: ризики, ресурси та результативність. Цифрова економіка та економічна безпека. 2025. Випуск 3(18). URL: https://dees.iei.od.ua/index.php/journal/article/view/740 DOI: https://doi.org/10.32782/dees.18-40

Ключові слова: ігрова індустрія, gamedev, ринок відеоігор, кібербезпека
Keywords: gaming industry, gamedev, video game market, cybersecurity

ВИКОРИСТАННЯ OPENDATA UKRAINE В ЦІЛЯХ OSINT

Бойко Віктор

кандидат технічних наук, доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Дручик Софія

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

У сучасному світі інформація є стратегічним ресурсом, який може визначати економічний, політичний та навіть військовий успіх держав і організацій. Одним із найважливіших напрямів роботи з інформацією є OSINT (Open Source Intelligence) – розвідка з відкритих джерел. Цей підхід дозволяє отримувати, аналізувати та інтерпретувати дані, які є у відкритому доступі, без використання засекречених або спеціальних каналів.

OpenData – це інформація, що генерується державою та оприлюднюється в машиночитаній формі для її подальшого використання бізнесом, громадськістю, журналістами, дослідниками та органами влади [1]. Відкриті дані – це в першу чергу можливість легкого, ефективного та стандартизованого обміну даними між усіма зацікавленими сторонами, в тому числі самими органами влади. Це дієвий механізм, який не лише “змушує” ділитися інформацією, але й допомагає отримувати дивіденди від цього. Основними ознаками інформації з відкритих джерел є те, що для її отримання не потрібно використовувати будь-які методи таємного збору, і що вона повинна бути отримана за допомогою засобів, які повністю відповідають авторським правам і комерційним вимогам постачальників, де це можливо". В Україні ключовою платформою є портал відкритих даних data.gov.ua, створений у рамках закону «Про доступ до публічної інформації». Він об’єднує тисячі наборів даних від різних органів державної влади та місцевого самоврядування [2].

OSINT (Open Source Intelligence) – це розвідка, заснована на аналізі відкритих джерел. Тобто всього, що є у вільному доступі: соціальні мережі, форуми, ЗМІ, державні реєстри, супутникові знімки, відео, бази злитих даних тощо. Простими словами – OSINT дозволяє знайти про людину або організацію максимум даних, не порушуючи закону. Це своєрідна легальна “розвідка”, але побудована не на хакерстві, а на аналітичному мисленні, досвіді і знанні джерел [3]. OSINT в основному використовується у функціях національної безпеки, правоохоронних органів та бізнес-розвідки, а також має цінність для аналітиків, які використовують неконфіденційні розвідувальні дані, що відповідають на секретні, несекретні або власні розвідувальні запити в рамках попередніх розвідувальних дисциплін [4].

У кібербезпеці OSINT може використовуватись як для захисту, так і для нападу. Ці техніки можуть допомогти у виявленні витоку даних. Часто хакери після зламу систем публікують частину вкрадених даних у згаданому вже даркнеті, щоб продемонструвати «товар». Якщо компанія вчасно зреагує, вона може запобігти подальшому розповсюдженню і зберегти недоторканність чутливих даних, які не входили до «демонстраційного пакету» [5].

Про відкриті дані в Україні всерйоз заговорили на початку 2013 року. Однією з перших ініціатив став проект Social Boost, що просуває концепцію відкритих даних і координує діяльність ентузіастів, IT-компаній та державних органів в Україні через соціально значимі IT-проекти, пов'язані з електронним урядом, електронної демократією, електронними послугами та відкритими урядовими даними. У 2014 році був розроблений законопроект про відкриті дані, прийнятий в першому читанні. Кабінет Міністрів розробив відповідну постанову про відкриття більш ніж 300 реєстрів і баз даних. У грудні 2017 року Кабінет міністрів України розширив перелік баз даних, які повинні публічно відкриватися державними органами, і кількість відкритих реєстрів зросла з 302 до 600. З 2013 по 2018 рік Україна поліпшила свою позицію в рейтингу Global Open Data Index. Наша країна стала однією з 50 найбільш відкритих держав, зайнявши 31-е місце. Точний розмір економічного потенціалу Open Data в даний час вивчається Київською школою економіки [6].

Серед ключових недоліків використання відкритих даних в Україні варто відзначити їхню неповноту, адже далеко не всі відомості, які мали б бути у відкритому доступі, представлені у відповідних реєстрах, а наявна інформація іноді подається лише частково. Проблемою є також некоректність відображення даних, коли в одному записі може міститися інформація про різних осіб або ж зазначаються помилкові ідентифікаційні коди юридичних осіб. Додаткові труднощі створює зміна стандартів даних, унаслідок чого змінюється структура чи формат публікацій, що призводить до збоїв у роботі автоматизованих сервісів і тимчасово обмежує користувачів у доступі до необхідної інформації. Важливою проблемою залишається і неактуальність даних, які не завжди оновлюються вчасно, а отже можуть бути застарілими або неточними. До цього додаються й технічні виклики, зокрема масовані кібератаки під час війни (особливо DDoS-атаки), що негативно впливають на стабільність роботи державних реєстрів та ускладнюють своєчасне отримання інформації користувачами [7].

Говорячи про переваги відкритих даних слід зазначити, що вони приносять грошову вигоду урядам і компаніям, скорочують витрати і покращують процеси прийняття рішень, створюють можливості для бізнесу і аналітиків даних. Open data здатна підвищувати прозорість та ефективність державного сектора, удосконалювати ділову практику, боротися з корупцією і ухиленням від податків. Сьогодні українці вже можуть отримувати і

використовувати тисячі файлів, опублікованих на data.gov.ua. Але багато громадян досі не знають про можливості відкритих даних. Поступово в Україні з'являється все більше можливостей використання опен дата: держава публікує інформацію, яка раніше була закрита, і підтримує проекти, спрямовані на використання відкритих даних [6].

Таким чином, використання відкритих даних в Україні у поєднанні з методами OSINT є потужним інструментом для підвищення прозорості, боротьби з корупцією та зміцнення інформаційної безпеки. Незважаючи на наявні недоліки – неповноту, неточність, неактуальність і технічні проблеми реєстрів – OpenData поступово розвивається і демонструє значний економічний та суспільний потенціал. Важливо, щоб держава і надалі вдосконалювала механізми публікації даних, а суспільство активніше використовувало їх у дослідженнях, бізнесі та сфері безпеки, адже саме у цьому полягає ключ до сталого розвитку й ефективної протидії сучасним викликам.

Список використаних джерел

1. Дія.Відкриті дані. URL: https://diia.data.gov.ua/info-center/wodi (дата звернення: 21.09.2025).
2. Що таке відкриті дані? – data.in.ua. data.in.ua. URL: https://www.data.in.ua/open-data/ (дата звернення: 21.09.2025).
3. OSINT - розвідка відкритих джерел: що це і чому варто замовити саме в Darkguard - DarkGuard. DarkGuard. URL: https://darkguard.com.ua/osint-rozvidka-vidkritih-dzherel-v-darkguard/ (дата звернення: 21.09.2025).
4. Maxym Z. Розвідка з відкритих джерел (Open-source intelligence - OSINT). Maxym Zosym. URL: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/ (дата звернення: 21.09.2025).
5. vkarpova7. Як працює osint-розвідка? Від бізнес-аналізу до оборони україни. ISSP Training. URL: https://www.issp.training/post/yak-pratsyuye-osint-rozvidka-vid-biznes-analizu-do-oborony-ukrayiny (дата звернення: 21.09.2025).
6. Open data в Україні. YouControl як частина open data ua. YouControl. URL: https://youcontrol.com.ua/topics/open-data-otkryityie-dannyie-youcontrol/ (дата звернення: 21.09.2025).
7. Недоліки держреєстрів в Україні, які ускладнюють роботу з даними. YouControl. URL: https://youcontrol.com.ua/articles/nedoliky-derzhreiestriv-v-ukrayini,yaki-uskladniuiut-robotu-z-danymy/ (дата звернення: 21.09.2025).

Ключові слова: інформація, OSINT, розвідка, відкриті дані, вільний доступ, data.gov.ua, національна безпека, державні реєстри, закон «Про доступ до публічної інформації», переваги відкритих даних, інформаційна безпека.
Keywords: information, OSINT, intelligence, open data, free access, data.gov.ua, national security, state registers, law "On Access to Public Information", advantages of open data, information security.

ЛОКАЛЬНИЙ МЕНЕДЖЕР ПАРОЛІВ ІЗ ГЕНЕРУВАННЯМ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Тимошенко Лідія

кандидат економічних наук, доцент кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»

Вакуліна Сана

здобувач кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»

Волобуєва Ірина

здобувач кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»

Із розвитком інформаційних технологій та масовим переходом до цифрових сервісів питання захисту облікових даних користувачів набуває особливої актуальності. Паролі є найпоширенішим методом автентифікації, однак користувачі часто обирають прості комбінації або повторюють ті ж паролі в різних акаунтах. Це призводить до підвищення ризику несанкціонованого доступу до персональних даних.

Надійність пароля безпосередньо залежить від його довжини, складності та ентропії. Для підвищення рівня безпеки важливо не лише створювати складні паролі, але й оцінювати їхню стійкість до підбору. Застосунок для автоматичного генерування паролів та оцінювання надійності сприяє формуванню звичок користувачів і підвищенню загального рівня кібербезпеки.

Метою роботи є забезпечення високої швидкості генерування паролів та конфіденційності процесів шляхом локального генерування і оцінювання їх надійності.

Під час проведення огляду сучасних програм для керування паролями – LastPass, Bitwarden, KeePass та 1Password, встановлено, що більшість орієнтовані на централізоване зберігання паролів у хмарних сховищах, що створює додаткові ризики витоку даних (табл. 1) [1]. Запропонований підхід – операції з обробки паролів виконуватимуться локально на пристрої користувача.

Таблиця 1 – Огляд програм для керування паролями

Назва	Основна ідея	Переваги	Недоліки
LastPass	Хмарний менеджер паролів. Зберігає зашифровані паролі, синхронізується між пристроями.	Зручний інтерфейс, багато функцій, автозаповнення, 2FA.	Мав витоки даних, залежність від мережі, лазівки безпеки (автозаповнення, браузерні плагіни) можуть бути вразливими.
Bit warden	Відкритий (open source) менеджер, з хмарною або самостійною (self-hosted) опцією.	Більше прозорості через відкритий код, можливість самостійного хостингу, сильне шифрування.	Деякі функції обмежені у безкоштовній версії; залежність від інтернету, якщо в хмарі; не всі частини інтерфейсу шифруються однаково у деяких менеджерах.
KeePass	Відкритий офлайн-менеджер. Дані зберігаються локально (файл бази), без необхідності серверів.	Повний контроль над даними, автономність, можна без мережі.	Менше зручностей (синхронізація через сторонні сервіси, ручне оновлення, UI), складніше для початківців.
1 Pass-word	Комбінація хмарного сховища й сильних еханізмів захисту, зручний інтерфейс, багатофакторна аутентифікація.	Нові високі стандарти безпеки, користувацький досвід, регулярні аудити, зручність + функції.	Часто платний, залежить від сервісів (хмарне зберігання), можуть бути витрати, якщо потрібно багато пристроїв або сімейний план.

Локальна система складається з трьох основних модулів.

1. Модуль генерації паролів:

– генерація рандомних комбінацій символів на основі заданих параметрів: довжина пароля, типи символів (літери, цифри, спеціальні знаки);

– можливість користувачу вказати потрібну довжину пароля;

– функція корекції згенерованого пароля користувачем.

2. Модуль оцінки надійності:

– перевірка введеного або згенерованого пароля за критеріями довжини, різноманітності символів та наявності повторів;

– використання списку з приблизно 200-от найпопулярніших паролів, які автоматично оцінюються як «слабкі»;

– результат оцінки надійності відображається у вигляді символів.

3. Модуль візуалізації результатів:

– відображення рівня надійності та ентропії пароля;

– надання рекомендацій щодо покращення пароля.

На рис. 1 наведено схему локального застосунку для генерування паролів від введення або генерації пароля, його модифікації, оцінки надійності до відображення результату користувачу.

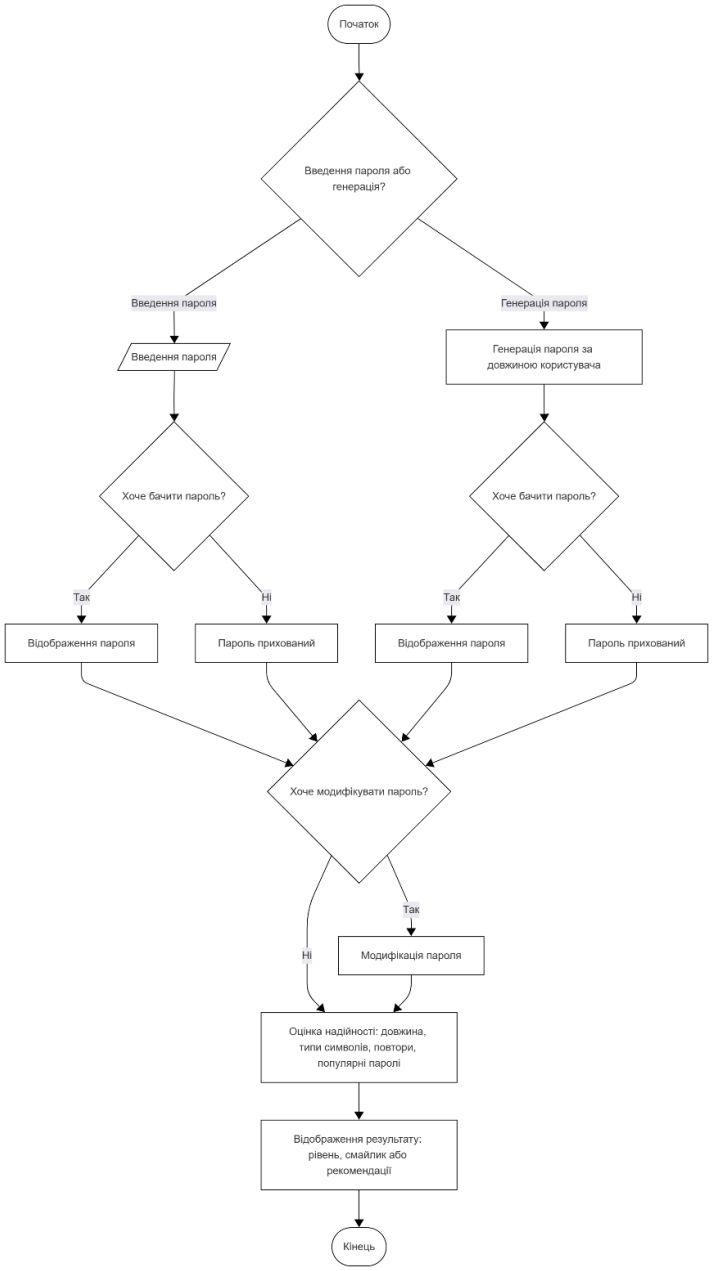

Рис.1. Схема локального застосунку для генерування паролів

Особливостями роботи системи є те, що всі обчислення виконуються локально на пристрої користувача, без обміну даними із зовнішніми сервісами, робота в офлайн-режимі для забезпечення безпеки та конфіденційності.

Розробку мобільного застосунку планується виконати у Android Studio з використанням мови Kotlin та фреймворку Android SDK для створення локального графічного інтерфейсу.

Для оцінки надійності пароля застосовуватимемо ентропійну модель, де рівень стійкості визначається за формулою [2]:

$$H = L \cdot log_2(N) \quad (1)$$

де L – довжина пароля,

N – кількість можливих символів у вибраному наборі.

На основі значення H пароль класифікують за рівнями стійкості:

– до 28 біт дуже слабкий;
– 28–36 біт слабкий;
– 36–60 біт середній;
– понад 60 біт сильний.

Результат оцінки відображатиметься користувачеві у графічній формі, наприклад, у вигляді смайлика або кольорового індикатора надійності.

Висновки. У результаті виконання роботи розроблено концепцію та прототип локального застосунку для генерування та оцінки надійності паролів на мобільних пристроях. Система працює автономно, без підключення до інтернету. Застосунок може бути інструментом навчання користувачів та частиною комплексних систем захисту інформації. Подальший розвиток проєкту – інтеграція модулів перевірки паролів за локальними словниками витоків, додавання рекомендацій із кібергігієни та впровадження адаптивних алгоритмів оцінювання на основі штучного інтелекту.

Список використаної літератури:

1. Alsharaya H. Password managers: a critical review of security, usability, and innovative designs. Journal of Computer Sciences Institute,2025, Т.36, №9, с. 28-35.
2. Oesch S., Ruoti S. Evaluating Password Managers Against Real-World Phishing Pages. IJCT Journal, 2025.

Ключові слова: пароль, застосунок, надійність, мобільний пристрій.
Keywords: password, application, reliability, mobile device

СУЧАСНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІНТЕЛЕКТУАЛЬНИХ ЖИТЛОВИХ СИСТЕМАХ

Неділенко Валерій

аспірант кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»

Вступ

Сучасні технології Інтернету речей (IoT) розвиваються з надзвичайною швидкістю, що створює нові виклики у сфері безпеки інформаційних систем. Одним із актуальних напрямів є захист розумних пристроїв та систем IoT, які активно інтегруються у побутові, промислові та енергетичні рішення. Пристрої IoT можуть містити різні бінарні дані, пов’язані з безпекою, для того щоб уможливити використання відповідних протоколів, наприклад, сертифікати

для безпечного зв'язку з віддаленими серверами (mqtt, http тощо). Зловмиснику, який має фізичний доступ до пристрою, дуже легко отримати бінарні образи зі сховища пристрою та шукати такі фрагменти тексту. Можливий витік сертифіката безпеки може призвести до ескалації атак на інші частини інфраструктури, особливо якщо відповідні дозволи є неправильними або досить послабленими.

Огляд літературних джерел

Серед сучасних підходів до забезпечення кібербезпеки IoT виділяють використання сертифікатів, криптографічних протоколів, механізмів автентифікації та постійного моніторингу. Зокрема, OWASP щорічно оновлює перелік найбільш критичних вразливостей для IoT-пристроїв [1]. Дослідники також розглядають постквантові методи шифрування [2], системи легковагової автентифікації для промислових застосувань [3] та технології керування сертифікатами для промислових мереж [4]. Автори [5] відзначають, що стандартні криптографічні методи не забезпечують повного захисту даних під час бездротової передачі в IoT. Перспективним підходом є обфускація сигналів - контрольоване спотворення даних, яке ускладнює їх перехоплення сторонніми особами. Ще одна цікава ідея представлена в роботі [6], де пропонується метод симуляції ідентифікаторів для пристроїв IoT. Завдяки цьому підходу можна визначати, до якої групи належить той чи інший об'єкт, і водночас ідентифікувати кожен пристрій у межах цієї групи.

Отже, хоча окремі методи, такі як криптографія, автентифікація чи обфускація, відіграють важливу роль у захисті конкретних ланок IoT-системи (наприклад, пристроїв, мереж чи даних), їх ефективність обмежена без комплексного підходу. Необхідно впроваджувати інтегровані стратегії, що охоплюють весь життєвий цикл системи - від апаратного рівня до хмарних сервісів, включаючи постійний моніторинг, оновлення вразливостей та комбінацію кількох технологій. Такий всебічний захист мінімізує ризики ланцюгових атак і забезпечує стійкість IoT-екосистеми в цілому, особливо в умовах зростання складності та взаємозв'язків сучасних мереж.

Цілі дослідження

Основною метою дослідження є розробка ефективного та надійного механізму захисту, що забезпечить безпеку зберігання та передачі даних від пристрою до хмарного сервісу AWS IoT Core.

Особлива увага приділена використанню сучасних методів шифрування та захисту від зламу для забезпечення конфіденційності, цілісності та доступності інформації. Щоб уникнути витоків, потрібно шифрувати пам'ять пристрою, щоб жодна конфіденційна інформація з образу мікропрограми або з іншого місця не могла бути прочитаної навіть за наявності фізичного доступу до пристрою.

Дослідження включає в себе не лише розробку апаратно-програмного комплексу, але й вивчення та аналіз відповідних аспектів кібербезпеки, зокрема у сфері захисту IoT-пристроїв від потенційних загроз та атак. Подальше вдосконалення та розширення можливостей захисту та взаємодії з AWS IoT Core є ключовими аспектами цього дослідження.

Методи та засоби

Для побудови безпечної системи IoT використано мікроконтролер ESP32 з операційною системою реального часу FreeRTOS. Застосовано шифрування енергонезалежної пам'яті (NVS), автентифікацію пристрою через сертифікати X.509 та взаємодію з AWS IoT Core за протоколом MQTT через захищене з'єднання TLS. Для оновлення програмного забезпечення реалізовано механізм OTA (Over-the-Air), що дозволяє дистанційно надсилати оновлення з перевіркою цілісності коду за допомогою цифрового підпису.

Результати дослідження

На рис.1 представлені методи захисту від кібератак, що реалізовані у роботі і які є відповідями на виклики TOP-10 OWASP IoT Vulnerabilities. Розроблена система інтегрується з хмарною платформою AWS IoT Core та забезпечує захищений обмін даними між пристроєм і сервером. Застосування апаратного шифрування пам'яті ESP32 унеможливлює отримання критичних даних навіть при фізичному доступі до пристрою.

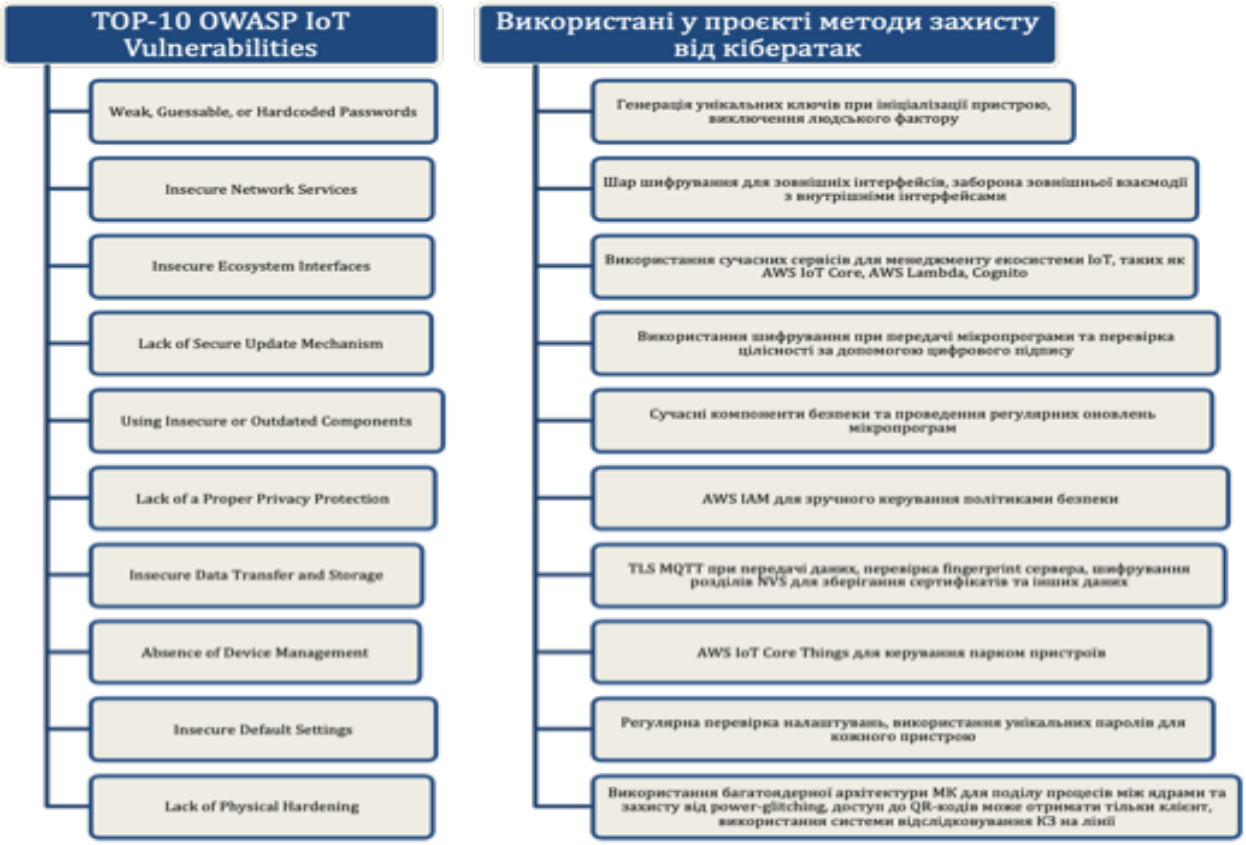

Рис.1. Відповідність між загрозами та реалізованими методами їх усунення

Для забезпечення належного рівня захисту IoT-системи від потенційних загроз було використано наступні ключові сучасні технології:

1. AWS IoT Core (хмарний шлюз для IoT пристроїв).
2. AWS IoT Core Shadow (створення постійної віртуальної версії кожного пристрою).
3. AWS Cognito (реєстрація та аутентифікація користувачів у мобільних та інтернет-додатках).
4. Центр ідентифікації AWS IAM Identity Center (сувора автентифікація на основі стандартів для всіх користувачів).
5. Amazon S3 Bucket (сервіс сховища).
6. Сервіс AWS Lambda (інструмент для керування кінцевими точками).
7. Сервіс AWS IoT Remote Jobs (завдання для набору пристроїв - завантаження та встановлення програм, запуск оновлень мікропрограм, зміна сертифікатів, операції дистанційного усунення несправностей).
8. AWS Signer (можливість підписання коду).
9. Операційна система реального часу FreeRTOS з відкритим кодом для мікроконтролерів.
10. Over-the-Air (оновлення мікропрограм).

Система дозволяє виконувати оновлення прошивки та керування пристроєм через мобільний додаток з обов'язковою автентифікацією користувача. Проведене тестування підтвердило стабільну роботу системи в умовах промислової експлуатації.

Висновки

У результаті виконання проєкту вдалося досягти важливих результатів у сфері захисту IoT-пристроїв. Розроблена система забезпечує високий рівень безпеки в зберіганні та передачі даних. Описана архітектура системи, взаємодія між AWS та ESP-IDF, а також методи шифрування та захисту від зламу для забезпечення безпеки зберігання та передачі даних. Детально проаналізовані технічні аспекти проектування, його інноваційні характеристики та взаємовідносини з вибраними технологічними рішеннями AWS та ESP-IDF. Перспективами подальших досліджень є розширення системи на інші галузі, зокрема медичну та критичну інфраструктуру.

Список використаних джерел:

[1] OWASP IoT Top 10 Vulnerabilities (2024 Updated). URL: https://www.wattle-corp.com/owasp-iot-top-10/.

[2] Zhang Y., Duan P., Li C., Ahmad H. Preserving Privacy of Internet of Things Network with Certificateless Ring Signature Sensors. Sensors (2025). doi:10.3390/s25051321.

[3] Al Ghazo A., Abu Mallouh M., Alajlouni S., Almalkawi I. Securing Cyber Physical Systems: Lightweight Industrial Internet of Things Authentication (LI2A). Appl. Syst. Innov. (2025). doi:10.3390/asi8010011.

[4] Göppert J., Walz A., Sikora A. A Survey on Life-Cycle-Oriented Certificate Management in Industrial Networking Environments. J. Sens. Actuator Netw. (2024). doi:10.3390/jsan13020026.
[5] Renato Lo Cigno, Francesco Gringoli, Stefania Bartoletti, Marco Cominelli, Lorenzo Ghiro, and Samuele Zanini. Communication and Sensing: Wireless PHY-Layer Threats to Security and Privacy for IoT Systems and Possible Countermeasures. Information 2025, 16(1), 31; https://doi.org/10.3390/info16010031.
[6] Volodymyr Maksymovych, Elena Nyemkova, Connie Justice, Mariia Shabatura, Oleh Harasymchuk, Yuriy Lakh and Morika Rusynko. Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators. Electronics 2022, 11(13), 2039; https://doi.org/10.3390/electronics11132039.

Ключові слова: безпека даних; AWS IoT Core; методи шифрування; кіберзахист IoT-пристроїв; апаратно-програмні рішення; ESP32; FreeRTOS.
Keywords: data security; AWS IoT Core; encryption methods; cybersecurity of IoT devices; hardware and software solutions; ESP32; FreeRTOS.

МЕТОД ФАКТОРИЗАЦІЇ ВЕЛИКИХ ЧИСЕЛ

Тимошенко Лідія
кандидат економічних наук, доцент кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»
Алєксєєва Софія
магістрант кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»

Забезпечення інформаційної безпеки є одним із ключових напрямів сучасної кібербезпеки. Особливе місце посідають асиметричні криптографічні системи, як RSA, надійність яких ґрунтується на складності задачі факторизації великих чисел. Проте з розвитком обчислювальної техніки та появою квантових технологій необхідне вдосконалення існуючих методів. Одним із перспективних підходів є модифікація методу Ферма, який є ефективним для близьких за значенням множників[1]. Його удосконалення може забезпечити підвищення ефективності криптоаналізу сучасних систем шифрування.

Метою дослідження є зменшення обчислювальної складності алгоритму факторизації великих чисел шляхом удосконалення класичного методу Ферма для оцінки криптостійкості RSA-подібних систем.

Факторизація великих чисел є однією з основних математичних задач, що забезпечує безпеку криптографічних систем з відкритим ключем [2]. Метод Ферма базується на представленні непарного числа як різниці двох квадратів $\boldsymbol{N = x^2 - y^2 = (x - y)(x + y)}$. Складність даного методу

оцінюється як *O(n(log2n)2)*. Метод простий для алгоритмічної реалізації, тому доцільно удосконалити його для можливої реалізації на звичайному комп'ютері для чисел великої довжини.

Перша ідея модифікації методу полягає у використанні системи обчислення в залишкових класах базису Крестенсона, яка дає змогу виконувати операції над меншими числами – лишками великих чисел, та без наскрізних переносів позиційних систем обчислень, що істотно знижує витрати обчислювальних ресурсів та скорочує час. У системи обчислень в залишкових класах всі операції є модульними.

Модифікований алгоритм містить перевірку можливості існування квадратного кореня за модулем з використанням символів Якобі. Це дозволяє відкидати значення, які не задовольняють умові існування кореня, і тим самим скорочує кількість ітерацій пошуку. Основними операціями алгоритму є пошук символа Якобі, перевірка чи добувається корінь квадратний за модулем та добування кореня від числа. Загальна складність розробленого алгоритму обчислюється як *O(nlog2n+2log22n+4n)» O(nlog2n)*. Отже, складність алгоритму зменшується з експоненційної до субекспоненційної для певного класу чисел.

Додатково система залишкових класів забезпечує паралельність обчислень: кожен модуль може оброблятись незалежно, що дозволяє реалізувати алгоритм на багатопроцесорних або кластерних системах.

Практична реалізація алгоритму виконана у середовищі C++ Builder, що дало змогу створити застосунок з графічним інтерфейсом для введення чисел, запуску факторизації та аналізу результатів. Тестування показало, що використання модифікованого методу скорочує час виконання у порівнянні з класичною реалізацією на 25–30 % при середніх значеннях модуля до 512 біт.

Висновки.Таким чином, отримана модифікація методу є перспективною для оцінки криптостійкості асиметричних систем та подальших досліджень у сфері оптимізації факторизаційних алгоритмів.

Список використаної літератури:

1. Wagon S. Fermat's Factoring Method. URL: http://mathworld. wolfram.com/FermatsFactorizationMethod.html
2. Timoshenko L., et al. Factorization algorithms for cryptographic analysis of asymmetric crypto systems. Informatics and mathematical methods in modeling, 2014, 4,№ 4: 342-348.

Ключові слова: криптографія, факторизація, система обчислень, лишки.
Keywords: cryptography, factorization, calculation system, remainders.

НОВІТНІ НАПРЯМИ РОЗВИТКУ СУЧАСНИХ БАЗ ДАНИХ

Щербина Юрій

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Ключову роль в управлінні зберіганням даних виконують системи управління базами даних (СУБД). Вони забезпечують ефективне систематизоване зберігання інформації і включають інструментарій підтримки її у актуальному стані. Оптимізація організації запитів в таких системах гарантує швидкодію процесів, пов'язаних з накопиченням даних та їх зберіганням у формальному вигляді, що дозволяє реалізацію процесів пошуку і аналізу інформації, і забезпечує ефективне управління цими процесами.

Традиційні підходи до створення баз даних та систем управління ними ґрунтувались на структурованому підході, найбільш відомим з яких є реляційна модель, запропонована Коддом [1]. Ця модель забезпечує надійну теоретичну основу для опису сутностей даних, їх атрибутів та взаємних зав'язків з використанням нормалізованих схем. На протязі десятирічь система управління реляційними базами даних (СУРБД) залишалась основним стандартом для програмних реалізацій, які не вимагають узгодження структурованих даних та підтримки транзакцій.

Поява великих швидкісних та різних за своїм форматом інформаційних середовищ, що вимагають аналітичного оброблення даних у реальному масштабі часу, а також хмарних технологій – зробили традиційну модель управління менш ефективною [2]. Фіксовані схеми, обмеженність можливості масштабування та жорстка нормалізація зменшують їх адаптацію до динамічних і напівструктурованих форматів даних. Саме через це, проектування баз даних поступово перейшло до розроблення більш гнучких розподілених інтелектуальних парадігм. Подальша еволюція проектування баз даних формувалась у напрямі розподілених гнучких та хмарно-орієнтованих архітектур.

На певному етапі було запропоновано нову архітектуру під назвою NoSQL (Not Only SQL). Вона надавала механізми зберігання та пошуку даних, що суттєво відрізнялись від традиційних реляційних баз даних, і мали гнучку схему, яка дозволяла просте горизонтальне масштабувуання та забезпечувала високу швидкість доступу в сучасних додатках [3]. Бази даних цього типу створювались для роботи з неструктурованими даними великих об'ємів. Закладена в їх основу гнучка модель даних та горизонтальна масштабованість робить їх вкрай зручними в новітніх хмарних проектах, де розподілення і розширення, а також швидкість доступу є пріоритетними вимогами.

Робота з нереляційними базами даних привела до появи новітніх мов запитів, самим відомим з яких є Cassandra Query Language (CQL). Запити, написані мовою CQL, підтримують такі бази даних, як Apache Cassandra, Scylla та DataStax Enterprise.

Сьогодні існує де-кілька різних архітектур баз даних типу NoSQL:

– Документо-орієнтовані бази даних, в яких дані зберігються у вигляді таких документів, як JSON або XML. Це такі бази даних як MongoDB, Couchbase та Firebase.

– Колонкові бази даних, в яких дані організовані у вигляді колонок, що забезпечує ефективне зберігання та аналіз великих обсягів інформації. До їх складу можна віднести такі бази, як Apache Cassandra та HBase.

– Графові бази даних, в яких використовується графова модель зберігання даних, яка забезпечуює високу ефективність під час роботи зі зв'язаними даними. Їх прикладами є Neo4j, Amazon Neptune та ArangoDB.

Бази даних перелічених типів забезпечують гнучкість (легке адаптування до різних типів інформації, масштабованість (дозволяють легко додавати нові вузли для обробки даних), продуктивність (мають високу швидкість доступу до даних та оброблення запитів).

Пізніше з’явились системи NewSQL, ціллю яких було об’єднання найкращих властивостей реляційних баз даних та баз даних NoSQL – можливості забезпечення масштабування без втрат узгодженості даних [4]. Вони уявляють собою важливий етап у розвитку інформаційних технологій і використовуються тоді, коли інформаційні потоки в системі перегружені, і необхідно забезпечення атомарності (Atomicity), узгодженості (Consistency), ізоляції (Isolation) і довговічності (Durability), тобто ACID-сумісності.

На відміну від NoSQL баз даних вони забезпечують більш високу продуктивність доступу до даних та швидкість обробки транзакцій, а також високу узгодженість даних, що робить їх придатними для додатків, де важлива цілісність даних, та мають можливість легко масштабувати базу даних.

Бази даних типу NewSQL використовуються у фінансових додатках при виконанні фінансових онлайн-платежів та у банківських транзакціях, де важливими є швидкодія та надійність. Вони також популярні у різноманітних інтернет-сервісах і онлайн-платформах для аналізу великих об’ємів даних та використання складних запитів.

Таким чином, на сьогодні, бази даних є невід'ємним інструментом, що забезпечує управління інформаційними ресурсами державних структур, приватних компаній та систем управління інфраструктурними об’єктами. Новітні технології баз даних, побудовані на основі архітектур NoSQL та NewSQL, включають хмарні рішення, які забезпечують гнучкість та масштабованість, а також аналіз великих даних (Big Data) для прийняття

обґрунтованих рішень на інтелектуальному рівні. Їх інтеграція з машинним навчанням та штучним інтелектом відкриває нові можливості для автоматизації та аналізу даних.

На даний час проблемою залишається достатньо велика різноманітність способів і підходів до зберігання і оброблення неструктурованих даних і, тому, у кожному окремому випадку, вибір інструментарію залежить від вимог конкретного проекту, його масштабу та характеристик даних.

Список використаних джерел:

1. E. F. Codd, “A relational model of data for large shared data banks,” Communications of the ACM, vol. 13, no. 6, pp. 377–387, 1970. : https://www.seas.upenn.edu/~zives/03f/cis550/codd.pdf
2. S. Tiwari, Professional NoSQL, John Wiley & Sons, 2011. URL : https://books. google.com.ua/books/about/Professional_NoSQL.html?id=tv5iO9MnObUC&redir_esc=y
3. Miral Borad, Tejas Chauhan, Harsh Mehta. A Review on NoSQL Databases. November 2017. International Journal of Science and Research (IJSR) 6(11): 26-28. URL : https://www.researchgate.net/publication/327883334_A_Review_on_NoSQL_Databases
4. Piekos, J. (2015). SQL vs, NoSQL vs. NewSQl: finding the right solution. Retrieved June, 11, 2018. URL : https://www.researchgate.net/publication/340978543_SQL_NewSQL_and_NOSQL_Databases_A_Comparative_Survey/link/5ec46445a6fdcc90d685d608/download?_tp=eyJjb250ZXh0Ijp7Im-ZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

Ключові слова: Системи управління базами даних, реляційна модель, хмарні технології, горизонтальне масштабування баз даних, нормалізація даних, напівструктурований формат даних.

Key words: Database management systems, relational model, cloud technologies, horizontal database scaling, data normalization, semi-structured data format.

ПРОБЛЕМА БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ У CRM-СИСТЕМАХ (НА ПРИКЛАДІ SALESFORCE)

Бойко Віктор

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Перепелиця Марія

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

CRM-системи стали ключовою інфраструктурою взаємодії бізнесу з клієнтами, оскільки централізують великі масиви персональних даних (ПД) –

від ідентифікаційних атрибутів до історії комунікацій і транзакцій. Саме тому безпека ПД у CRM є не лише технічною задачею, а й предметом правового регулювання, корпоративного управління ризиками та відповідальності перед клієнтами. Особливості сучасних CRM як хмарних багатокористувацьких рішень (multi-tenant), їхня широка інтегрованість через API, мобільні клієнти та маркетингові екосистеми створюють розгалужену поверхню атаки і множину сценаріїв витоків даних. У роботі розглядаються характерні загрози та організаційно-технічні механізми їхнього стримування на прикладі Salesforce, однієї з найпоширеніших CRM-платформ, з опорою на офіційні навчальні матеріали Trailhead [1], [2].

Актуальність проблеми зумовлена концентрацією ПД у CRM та зростанням залежності бізнес-процесів від цих платформ. Будь-яка помилка конфігурації доступу, некоректна інтеграція або неналежне управління життєвим циклом ПД можуть призвести до інцидентів, що мають фінансові, репутаційні й юридичні наслідки (у т.ч. штрафи за порушення GDPR та національного законодавства). Для великих організацій, де CRM інтегрує відділи продажів, підтримки, маркетингу та аналітики, вразливість одного сегмента здатна спричинити каскадні ефекти у суміжних, подовжуючи час відновлення сервісів та збільшуючи сукупні втрати – отже, міркування стійкості та швидкого відновлення мають бути невід'ємною частиною моделі захисту [9]-[14].

Проблематика безпеки ПД у CRM має декілька рівнів. Технічний рівень охоплює моделі доступу до даних і шифрування, аудит подій, сегментацію середовища та керування інтеграціями. Організаційний рівень визначає політики мінімізації даних, принцип «найменших привілеїв», контроль постачальників (включаючи додатки з маркетплейсів), навчання користувачів і процедури реагування. Правовий рівень регламентує правові підстави обробки, інформування суб'єктів, права доступу/видалення, транскордонні передачі та локалізацію даних. У хмарних CRM ці рівні взаємозалежні: наприклад, вибір регіону розміщення даних (data residency) безпосередньо впливає на можливість дотримання локальних норм та на архітектурні рішення резервування й відновлення [9]-[13], [15].

На прикладі Salesforce можна системно описати основні вектори ризику та механізми їхнього пом'якшення. Базовою умовою є правильна побудова моделі доступу: організаційні стандартні налаштування (Organization-Wide Defaults), ієрархія ролей (Role Hierarchy) та правила надання доступу (Sharing Rules) працюють разом і визначають, хто і що бачить у межах організації. Ієрархія ролей надає менеджерам видимість записів підлеглих, а правила шерингу дозволяють робити винятки та розширювати доступ поза ієрархією – у т.ч. для зовнішніх користувачів-партнерів. Правильне застосування цих механізмів, разом із контролями доступу на рівні полів (Field-Level Security) та

об'єктів (Profiles/Permission Sets), формує «базову лінію» захисту ПД та мінімізує ризики надмірних прав користувачів [1]-[4], [14].

Шифрування даних у стані спокою – ключова вимога для ПД, що зберігаються у хмарі. У Salesforce ця функція реалізується через Shield Platform Encryption, яка дозволяє шифрувати конфіденційні поля та файли з керуванням життєвим циклом ключів. Для організацій, що опрацьовують ПД високої чутливості (фінансова/медична інформація, ідентифікаційні документи), увімкнення шифрування «на місці зберігання» поряд із політиками маскування даних у непроходових середовищах (Data Mask) знижує наслідки компрометації та обмежує видимість ПД навіть для привілейованих користувачів [5], [6].

Моніторинг і аудит – ще один критичний шар захисту. Подієвий моніторинг (Event Monitoring) надає журнали дій користувачів і клієнтів API, що дозволяє виявляти аномалії (масове завантаження даних, підозрілі логіни, нетипові запити) і будувати дашборди для оперативного реагування. Реалізація моніторингу у реальному часі та застосування політик транзакційної безпеки (Transaction Security) допомагають не лише «бачити» події, а й запобігати небажаним діям (наприклад, блокувати скачування великого обсягу ПД поза графіком) [7], [8].

Проблеми безпеки ПД у CRM часто походять від інтеграцій і додатків. Salesforce як платформа підтримує численні з'єднання через API та екосистему додатків, що створює ризики поширення доступів і копій ПД за межі контрольованого периметра. Політики «need-to-know», ревізія маркерів/секретів, обмеження обсягу даних у вебхуках та регулярний перегляд дозволів додатків мають бути обов'язковими; контроль повинен підкріплюватися технічними засобами – від журналів подій API до лімітів запитів і автоматизованих сповіщень про нетипові інтеграційні патерни. З огляду на мобільні клієнти та віддалений доступ, доцільно застосовувати умовний доступ (policy-based) і обмеження експорту ПД у незахищені канали [1], [7], [8].

Важливим напрямом зниження ризиків є управління життєвим циклом ПД і мінімізація даних. Модуль Privacy Center у Salesforce дозволяє створювати політики зберігання, маскування й видалення ПД та підтримувати запити суб'єктів даних (копія, стирання, знеособлення). Коректна класифікація ПД (визначення категорій чутливості й призначення відповідних контролів доступу) покращує узгодженість політик і спрощує доведення відповідності регуляторним вимогам. У межах продуктової лінійки Salesforce також доступні засоби виявлення ПД (Data Detect) і навчальні матеріали з політик приватності, що формують методичну основу для впровадження «privacy by design» [9]-[11].

Окремо варто відзначити вимоги локалізації та резидентності даних. Ініціатива Hyperforce дає змогу обирати регіон зберігання даних і підтримувати

локальні вимоги, забезпечуючи зберігання ПД «на місці» в публічній хмарі та спрощуючи відповідність нормам (у т.ч. GDPR і національним). Для організацій із географічно розподіленою присутністю коректна стратегія резидентності зменшує юридичні ризики і спрощує моделювання відмовостійкості [12], [13].

З урахуванням наведеного, ключові групи ризиків у CRM можна структуровано подати так:

- Конфігураційні: помилки у ролях/правах, надмірні дозволи, «приватні» об'єкти без винятків, або, навпаки, надто широкі правила доступу [1].
- Інтеграційні: витоки через API/вебхуки, слабкі секрети, додатки третьої сторони, що запитують надмірні скоупи [7], [8].
- Операційні: масові експорти, відсутність журналювання, несвоєчасний аналіз подій, відсутність тригерів реального часу [7], [8].
- Дані та приватність: відсутність політик мінімізації, неточна класифікація, зберігання ПД у непотрібних середовищах, відсутність автоматизованого видалення/маскування [9]-[11].
- Юридичні: неврегульовані транскордонні передачі, відсутність прозорих підстав обробки, порушення строків відповіді на запити суб'єктів [9]-[13].

Практична модель підвищення безпеки ПД у Salesforce повинна поєднувати архітектурні та процесні заходи. На архітектурному рівні: визначити «зону довіри» для ПД, застосувати Shield Platform Encryption до чутливих полів/файлів, установити політики Data Mask у непроходових середовищах, упровадити шаблон «least privilege» з регулярними recertification-кампаніями прав доступу; окремо – уніфікувати правила шерингу, мінімізувати індивідуальні винятки. На рівні моніторингу: активувати Event Monitoring (у т.ч. реального часу) та Transaction Security, налаштувати дашборди ризикових подій (аномальні logins, великі експорти, масштабні API-виклики). На рівні даних і приватності: запровадити класифікацію ПД і політики Privacy Center для автоматизованої мінімізації, видалення та обробки запитів суб'єктів даних; підтримувати data lineage для інтеграцій. На організаційному рівні: затвердити політики екосистеми додатків, провести інвентаризацію інтеграцій, обмежити скоупи доступів, установити процеси безпечного розроблення (DevSecOps) для конфігурацій і метаданих CRM. На рівні стійкості: поєднати резервне копіювання/відновлення з репетиціями інцидент-response, щоб скорочувати час відновлення та уникати каскадних збоїв у суміжних сервісах [5]-[11], [16].

Висновки. Безпека ПД у CRM-системах – це системна задача на перетині технічних, організаційних і правових практик. На прикладі Salesforce видно, що платформа надає розвинуті механізми керування доступом,

шифрування, моніторингу подій та управління приватністю. Однак ефективність цих механізмів визначається якістю їхнього впровадження: узгодженістю ролей і правил шерингу, дисципліною в інтеграціях, наявністю політик класифікації/мінімізації даних і постійним аудитом. З огляду на зростання обсягу й цінності ПД, а також на правові вимоги, організації мають інвестувати в налаштування та періодичну перевірку захисних контролів, а також у підготовку користувачів. Для студентів і фахівців із кібербезпеки Trailhead-пісочниці (Trailhead Playgrounds) дають безпечне середовище відпрацювання цих підходів без доступу до продуктивних даних – це дозволяє формувати практичні навички без витягання коду з реальної CRM та без ризику для ПД [1], [2].

Список використаних джерел:

1. Data Security – Improve Record Access Control in Your Org. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/data_security/data_security_records
2. Trailhead Playground Management – Module. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/trailhead_playground_management
3. Define Sharing Rules. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/data_security/data_security_sharing_rules
4. Communities & External Users – Sharing Rules. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/projects/communities_share_crm_data/sharing_rules
5. Shield Platform Encryption. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/spe_admins
6. Shield Platform Encryption – Quick Look. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/shield-platform-encryption-quick-look2/get-to-know-shield-platform-encryption2
7. Event Monitoring – Module. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/event_monitoring
8. Real-Time Event Monitoring – Module. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/realtime-event-monitoring
9. Privacy Center – Module. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/privacy-center
10. Prepare for Privacy Center. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/privacy-center/prepare-for-privacy-center
11. Create a Data Management Policy in Privacy Center. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/privacy-center/create-a-data-management-policy-in-privacy-center
12. Hyperforce – Data Residency. Salesforce Help. URL: https://help.salesforce.com/s/articleView?id=000795008
13. Introducing Hyperforce – General Information & FAQ. Salesforce Help. URL: https://help.salesforce.com/s/articleView?id=000388902

14. Create a Role Hierarchy. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/data_security/data_security_roles
15. Cybersecurity Challenges in Cloud-based CRM. SSRN Working Paper, 2024. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5005031
16. Best Practices for Protecting Your CRM Data. National Cybersecurity Alliance (StaySafeOnline), 2025. URL: https://staysafeonline.org/articles/best-practices-for-protecting-your-crm-data

Ключові слова: CRM, персональні дані, конфіденційність, доступ на основі ролей, правила шерингу, шифрування, моніторинг подій, Privacy Center, Hyperforce, резидентність даних.
Keywords: CRM, personal data, confidentiality, role-based access, sharing rules, encryption, event monitoring, Privacy Center, Hyperforce, data residency.

ЗАХИСТ ІГРОВИХ РЕСУРСІВ У СУЧАСНИХ ВІДЕОІГРАХ: КОНЦЕПЦІЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ В ГРІ «HONEY & MOLD»

Дяченко Аріна

студентка 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Соколов Артем

доктор технічних наук, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»

Сфера відеоігор є однією з найдинамічніших і фінансово потужних галузей цифрової індустрії: щороку ігровий ринок залучає мільярдні інвестиції та забезпечує значні прибутки розробникам, видавцям і сервісним платформам. В умовах такої конкуренції успіх ігрового продукту значною мірою залежить від ефективності механізмів захисту внутрішніх ресурсів [1, 2]. Порушення цілісності ігрових даних, втручання у збереження, маніпуляції з внутрішньою економікою чи обхід механік прогресу можуть не лише руйнувати баланс гри, але й завдавати прямих фінансових збитків.

Сучасні відеоігри давно вийшли за межі традиційних розваг і перетворилися на складні програмні системи, в яких поєднуються елементи кібербезпеки, управління даними, штучного інтелекту та мережевої інфраструктури. Тому захист внутрішніх ігрових ресурсів стає критично важливим завданням і для великих студій, і для розробників. Особливо актуальним це є у проєктах, де економічний баланс визначає динаміку геймплею й безпосередньо впливає на користувацький досвід.

Метою цієї роботи є проєктування системи безпеки ресурсів гри «Honey & Mold».

У даній роботі розглянуто концепцію та реалізацію ігрового проєкту «Honey & Mold» – стратегії з елементами виживання, в якій гравець керує бджолиною маткою, що має відновити свій улей, збираючи ресурси, формуючи черги робочих бджіл і створюючи спеціальні костюми для подолання перешкод. Гра поєднує механіки управління чергами завдань, систему життєвих циклів робочих бджіл, крафт та наративні елементи у вигляді лже-артефактів, що розкривають приховану історію світу.

У процесі розробки ігрового проєкту особливого значення набуває визначення ресурсів, що є критичними для ігрової економіки та, відповідно, становлять підвищений ризик несанкціонованої модифікації. У грі «Honey & Mold» таким ресурсом є мед, який виступає базовою внутрішньоігровою валютою, впливає на прогрес, баланс і доступність ігрових механік. Тому захист цілісності даного ресурсу потребує окремого технічного забезпечення.

Найпоширенішими загрозами для подібних ресурсів виступають:

– пряме редагування локальних значень у пам’яті під час виконання гри;

– маніпуляції файлами збережень;

– модифікація кінцевих станів за допомогою утиліт на кшталт Cheat Engine;

– застосування спеціальних «тренерів», що змінюють логіку виконання окремих функцій, перехоплюють виклики API або підміняють параметри гри під час роботи.

Для запобігання таким атакам у проєкті застосовується кілька взаємодоповнювальних механізмів:

1. Центральним елементом захисту є система локальних збережень на основі SQLite із криптографічним шифруванням полів та вбудованим хеш-значенням, що підписується за допомогою секретного ключа. Під час кожного завантаження даних гра здійснює перевірку відповідності хеш-значення, підписаного ключем, що зберігається у програмі [3]; у разі виявлення відмінностей дані розглядаються як модифіковані, а система або відновлює коректний стан з резервної копії, або ініціює захисну реакцію, наприклад, сповіщення користувача чи блокування підозрілих змін.

2. Щоб унеможливити підроблення лише підсумкових значень, використовується подвійний журнал транзакцій із незворотною моделлю дописування, а також механізм відновлення action-log, який дозволяє відтворити повну історію операцій та перевірити достовірність фінального стану через детерміністичне виконання подій. Такий підхід суттєво ускладнює втручання в економіку гри навіть при використанні інструментів на кшталт Cheat Engine, оскільки зміна одного лише числового значення не відповідає транзакційній історії та неминуче призводить до виявлення невідповідності.

3. Для протидії тренерам, що працюють через ін'єкцію коду або підміну функцій, застосовуються перевірки цілісності виконуваного коду, контроль сигнатур основних DLL, періодична валідація критичних функцій з використанням обфускації та випадкових структур даних, а також часткове перенесення логіки перевірки ресурсів у приховані внутрішні модулі, що динамічно генеруються під час виконання.

Комплексне застосування цих механізмів, посилене телеметричним моніторингом через Steamworks API, забезпечує надійний захист ключових ігрових ресурсів і підтримує стабільність внутрішньоігрової економіки навіть за умов активних спроб маніпуляції з боку користувачів.

Запропонована система захисту ігрових ресурсів відеогри «Honey & Mold» демонструє ефективність поєднання криптографічних методів, журналювання транзакцій та перевірок цілісності коду для запобігання несанкціонованим змінам локальних даних та обходу внутрішньоігрової логіки. Водночас запропоновані підходи є масштабованими та можуть бути адаптовані для інших ігрових проєктів із різними жанрами та моделями економіки, забезпечуючи стабільність внутрішньоігрових систем і захист критичних ресурсів.

Перспективними напрямами подальших досліджень є проведення практичного тестування ефективності описаних механізмів на різних платформах, оцінка стійкості проти сучасних інструментів для модифікації пам'яті, інтеграція методів машинного навчання для автоматичного виявлення потенційних атак та аномалій у поведінці користувачів, а також розробка спеціалізованих криптографічних алгоритмів, адаптованих для роботи з іграми. Таке поєднання теоретичних та практичних підходів дозволяє підвищити надійність ігрових систем та формує основу для подальшого розвитку досліджень у сфері кібербезпеки відеоігор.

Список використаної літератури:

1. Huang J. et al. Improved Public-Key Searchable Encryption Scheme for Cloud-Based Responsible Gaming Systems. Cross Strait Radio Science and Wireless Technology Conference (CSRSWTC). IEEE, 2024. P. 1-3.
2. Lukas M., Tomicic I., Bernik A. Anticheat system based on reinforcement learning agents in unity. Information. 2022. Vol. 13, No. 4. P. 173.
3. Mohammed Q. A. A. S., Joudah M., Mohammed H. A survey on digital signature schemes. AIP Conference Proceedings. AIP Publishing LLC, 2024. Vol. 3232. No. 1. P. 020057.

Ключові слова: захист даних, відеоігри, шифрування, хешування, локальна база даних, кібербезпека.
Keywords: data protection, video games, encryption, hashing, local database, cybersecurity.

АЛГОРИТМІЧНІ ПІДХОДИ ДО ПІДТВЕРДЖЕННЯ АВТОРСТВА ТА ЦІЛІСНОСТІ МУЛЬТИМЕДІЙНИХ ДАНИХ

Овчинников Микола

асистент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Захист інтелектуальної власності на мультимедійні дані у кіберпросторі ускладнюється тим, що контент легко копіюється й модифікується, а типові перетворення (компресія, перекодування, зміна роздільності, кадрування) можуть знищувати або спотворювати ознаки авторства. Для правовласника важливі не лише виявлення копій, а й доказовість результатів: відтворюваний ланцюжок обробки, контроль цілісності артефактів та можливість аудиту, що напряму пов'язано з алгоритмічними та технічними аспектами кібербезпеки. [2,5]

У межах досліджень розробляється підхід до інформаційної системи, що поєднує робастне водяне маркування, перцептивне хешування/фінгерпринти та незмінний журнал подій (permissioned blockchain або WORM-лог). Комбінація цих компонентів зменшує ризик «однієї точки відмови»: водяний знак забезпечує вбудовану атрибуцію, перцептивні ознаки підтримують масштабований пошук, а журнал підвищує незаперечність і прозорість процедури перевірки. [1,3,2]

Алгоритмічний конвеєр включає нормалізацію контенту (уніфікація параметрів кодування, стабілізація яскравості/контрасту; для відео – ключові кадри; для аудіо – спектральні «відбитки»), формування стійкого опису об'єкта (перцептивний хеш та додаткові ознаки), а також вбудування водяного знаку у частотній області (DCT/DWT) з адаптивним добором сили вбудування. Для доказовості результати (ідентифікатор контенту, хеші, параметри маркування, часові мітки) підписуються та реєструються у незмінному журналі разом із протоколами перевірок. [3,4]

Загрозна модель охоплює стирання/спотворення маркування, геометричні перетворення, часткове використання (колажі, ремікси), а також атаки на доказовість (підробка журналів, компрометація ключів). Протидія реалізується багатоканально: поєднанням робастного маркування, незалежних ознак схожості, криптографічного підпису та контрольованого доступу (ролі, MFA, принцип найменших привілеїв). Оцінювання ефективності пропонується проводити через ймовірність детекції знаку після перетворень, точність пошуку (precision/recall) і помилки прийняття рішень (FAR/FRR) для порогів схожості; узагальнення наведено у табл. 1 і на рис. 1. [1,3]

Практична реалізація контуру вимагає узгодження параметрів між модулями: для водяних знаків — вибір домену вбудування (DCT/DWT), сили сигналу та секретного ключа; для перцептивних ознак — нормалізація,

квантування й побудова індексів близькості. У результаті формується компактний «відбиток» контенту, придатний для індексації та аудиту без розкриття первинних даних, а також забезпечується трасованість операцій у межах життєвого циклу мультимедійного об'єкта [1].

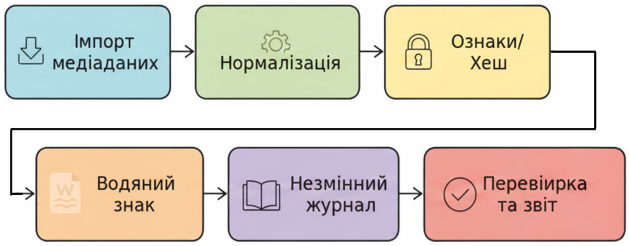

Рис. 1. Узагальнена схема алгоритмічного контуру.

Схема на рис. 1 відображає «ланцюжок довіри»: кожен етап формує артефакти (хеші, параметри маркування, часові мітки, підписи), які зберігаються разом із посиланням на медіаоб'єкт. Важливо, що ці артефакти мають бути достатніми не лише для підтвердження факту перевірки, а й для її повторення іншою стороною за тим самим протоколом (версії алгоритмів, пороги рішень, параметри препроцесингу). Такий підхід забезпечує відтворюваність процедури верифікації, дозволяє локалізувати етап, на якому виникла аномалія (наприклад, деградація водяного знака після перекодування або «дрейф» перцептивних ознак після генеративної модифікації), і підвищує доказовість результатів під час інцидентного аналізу або експертизи. Додатковою перевагою є можливість формування узгодженого «пакета доказів» для взаємодії з платформами чи судовими інстанціями: посилання на джерело, таймлайн подій, результати витягування маркера та метрики схожості. За умови незмінного журналювання (WORM/permissioned-реєстр) зменшується ризик підміни або ретроспективного редагування даних перевірки, що критично для процедур, де потрібна простежуваність та аудит дій користувачів [2, 5].

Наведене у таблиці 1 узагальнення дозволяє формалізувати відповідність «атака — контрзахід — метрика/критерій» та використовувати ці показники для налаштування порогів схожості й регламентів перевірки у практичних сценаріях (пошук копій, доведення авторства, аудит змін) [1, 3, 4].

Запропонований комплекс дає змогу будувати відтворюваний «пакет доказів» (артефакти, параметри, метрики, посилання на записи журналу) та підвищує стійкість захисту прав на мультимедійні дані в умовах типових кіберзагроз. Перспективними напрямами є підвищення стійкості до генеративних модифікацій (deepfake), оптимізація пошуку у великих колекціях (ANN-індекси) та формалізація ризик-орієнтованих показників ефективності впровадження.

Таблиця 1. Загрози та технічні контрзаходи (узагальнено). Джерело: авторська розробка.

Загроза	Атака	Контрзахід	Метрика/критерій
Стирання маркування	Компресія, фільтрація, перекодування	Робастне вбудування у DCT/DWT; адаптивна сила	Pdet після перетворень
Геометричні зміни	Кадрування, поворот, ресайз	Нормалізація; синхронізуючі шаблони/інваріантні ознаки	Стійкість до Δмасштабу/Δкута
Часткове використання	Колаж, ремікс, підміна фрагментів	Перцептивні ознаки + пошук за близькістю; сегментація	Precision/Recall (пошук)
Підробка доказів	Зміна журналів, компрометація ключів	Незмінний журнал + підпис; контроль доступу (ролі, MFA)	Аудит, незаперечність

Для компонента робастного маркування доцільно застосовувати частотні методи (DCT/DWT) із адаптивним вибором сили вбудування, що підвищує стійкість до компресії та фільтрації при мінімальній помітності. Параметри маркування (ключ, домен, коефіцієнт) фіксуються у доказовому пакеті та підписуються, а ефективність оцінюється за метриками непомітності (PSNR/SSIM) і ймовірності детекції після перетворень (Pdet). [1]

Перцептивне хешування та мультимодальні «фінгерпринти» забезпечують пошук збігів у великих колекціях за принципом близькості, а не біт-в-біт. Для зменшення помилкових спрацювань комбінуються кілька типів ознак, а пороги добираються за результатами валідації (ROC/EER) з контролем FAR/FRR; підозрілі збіги підтверджуються повторною перевіркою наявності водяного знака. [3,4]

Незмінний журнал подій реалізується як WORM-сховище або permissioned blockchain із хеш-ланцюжком та деревами Меркла для підтвердження цілісності. У журналі зберігаються хеші, перцептивні відбитки та метадані (без розміщення медіаданих), що підвищує конфіденційність. Захист посилюється керуванням ключами, рольовим доступом і MFA; метрики верифікації можуть передаватися до SIEM/SOAR для інцидентних сповіщень. [2,5].

Список використаних джерел:

1. Mekhfioui M., El Bazi N., Laayati O., et al. Optimized Digital Watermarking for Robust Information Security in Embedded Systems. Information. 2025;16(4):322. https://doi.org/10.3390/info16040322.
2. Qureshi A., Megías Jiménez D. Blockchain-Based Multimedia Content Protection: Review and Open Challenges. Applied Sciences. 2021;11(1):1. https://doi.org/10.3390/app11010001.
3. Du L., Ho A.T.S., Cong R. Perceptual hashing for image authentication: A survey. Signal Processing: Image Communication. 2020;81:115713. https://doi.org/10.1016/j.image.2019.115713.

4. Xing H., Wang Y., Xia L., He M. Image perceptual hashing for content authentication based on Watson's visual model and locally linear embedding. Journal of Real-Time Image Processing. 2023;20:7. https://doi.org/10.1007/s11554-023-01269-9.
5. Xiao X., He X., Zhang Y., et al. Blockchain-based reliable image copyright protection. IET Blockchain. 2023;3(4):222–237. https://doi.org/10.1049/blc2.12027.

Ключові слова: кібербезпека, інтелектуальна власність, мультимедійні дані, цифровий водяний знак, перцептивний хеш, блокчейн, форензіка.
Keywords: cybersecurity, intellectual property, multimedia data, digital watermark, perceptual hash, blockchain, forensics.

Науковий керівник: к.т.н., доцент Ахмаметьєва Г.В.

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ КІБЕРБЕЗПЕКИ В ОНЛАЙН ТА ОФЛАЙН ІГРАХ

Скідан Владислав
аспірант кафедри кібербезпеки Національного університету «Одеська юридична академія»

У сфері комп'ютерних ігор кібербезпека набуває все більшого значення через стрімкий розвиток технологій та зростання аудиторії гравців, які взаємодіють з віртуальними середовищами. Онлайн-ігри, що передбачають постійне підключення до мереж, стикаються з широким спектром загроз, таких як DDoS-атаки, фішинг та витоки даних, тоді як офлайн-ігри, орієнтовані на локальне виконання, більше схильні до ризиків, пов'язаних з піратством, шкідливим програмним забезпеченням у модифікаціях чи несанкціонованим доступом до локальних файлів. Порівняльний аналіз методів кібербезпеки в цих двох типах ігор дозволяє виявити спільні та відмінні підходи до захисту, підкреслюючи необхідність адаптації стратегій до специфіки середовища. Зокрема, в онлайн-іграх акцент робиться на мережевому рівні захисту, тоді як в офлайн-іграх переважають локальні механізми аутентифікації та контролю цілісності файлів.

У онлайн-іграх методи кібербезпеки часто включають багатошарові системи захисту, такі як шифрування даних для запобігання витокам інформації, багатофакторну аутентифікацію для захисту акаунтів гравців та системи виявлення ботів і читів, які використовують фаєрволи та CAPTCHA для блокування автоматизованих атак. Наприклад, DDoS-атаки, що перевантажують сервери та призводять до простоїв, вимагають впровадження спеціалізованих інструментів моніторингу трафіку, які аналізують аномалії в реальному часі та автоматично перенаправляють шкідливий трафік. Крім того, для боротьби з соціальною інженерією, такою як фішинг через ігрові чати, застосовуються освітні кампанії та автоматизовані фільтри контенту, що сканують повідомлення на наявність шкідливих посилань. Ці методи не лише захищають дані гравців, але й забезпечують

справедливість ігрового процесу, запобігаючи маніпуляціям з віртуальними активами, які можуть бути продані за реальні гроші. Дослідження показують, що ефективність таких підходів зростає при інтеграції з хмарними сервісами, де дані зберігаються в зашифрованому вигляді, зменшуючи ризики масових витоків, як це спостерігалося в інцидентах з великими платформами [1].

На противагу цьому, в офлайн-іграх методи кібербезпеки зосереджені на локальному рівні, де ключовими є системи цифрового управління правами (DRM), такі як Denuvo чи Steam DRM, які запобігають піратству шляхом перевірки ліцензій та блокування несанкціонованих копій. Ці системи часто включають офлайн-аутентифікацію, де гра періодично перевіряє цілісність файлів за допомогою хеш-функцій, щоб виявити модифікації чи вбудоване шкідливе ПЗ. Крім того, для захисту від вірусів у завантажених модифікаціях застосовуються вбудовані антивірусні модулі або рекомендації щодо використання зовнішнього ПЗ для сканування файлів перед установкою. У порівнянні з онлайн-іграми, тут менше уваги приділяється мережевим загрозам, але акцент робиться на запобіганні локальним вразливостям, таким як ін'єкції коду в збережені файли чи експлойти в одиночних режимах. Дослідження підкреслюють, що офлайн-ігри менш вразливі до масових атак, але ризики зростають при використанні піратських версій, де шкідливе ПЗ може бути замасковане під гру [2].

Порівнюючи методи в онлайн та офлайн іграх, можна відзначити, що в онлайн-середовищі переважають динамічні системи моніторингу, такі як AI-виявлення аномалій для боротьби з читами та ботами, тоді як в офлайн-іграх статичні перевірки, як хешування файлів, забезпечують базовий захист. Онлайн-ігри часто інтегрують VPN-рекомендації для маскування IP-адрес гравців, запобігаючи доксінгу чи светінгу, чого не потребують офлайн-ігри, де загрози обмежуються локальним пристроєм. Однак спільним для обох є використання сильних паролів та оновлень ПЗ для закриття вразливостей. Актуальні дослідження вказують на те, що гібридні ігри, які поєднують онлайн та офлайн елементи, вимагають комбінованих методів, де локальний DRM доповнюється мережевим шифруванням для захисту збережень у хмарі. Це дозволяє мінімізувати ризики, пов'язані з переходом між режимами, і підвищує загальну стійкість системи [3].

Відмінності у методах кібербезпеки наведено в таблиці 1.

У контексті офлайн-ігор методи кібербезпеки еволюціонували від простих ключів активації до складних систем, таких як вбудовані античити в одиночних кампаніях, які перевіряють модифікації на сумісність та безпеку. Наприклад, ігри на зразок тих, що використовують Unity чи Unreal Engine, інтегрують локальні скрипти для виявлення змін у коді, запобігаючи ін'єкціям шкідливого вмісту. Порівняно з онлайн, де загрози динамічні та вимагають постійного моніторингу, офлайн-методи більш пасивні, але ефективні для

збереження інтелектуальної власності. Дослідження зазначають, що в офлайн-режимах ризики часто пов'язані з користувацькими помилками, такими як завантаження з ненадійних джерел, тому рекомендації включають використання офіційних магазинів та регулярні оновлення. Це підкреслює необхідність освітніх елементів навіть у локальних іграх, де гравці можуть не усвідомлювати загроз [4].

Таблиця 1 – Аналіз методів кібербезпеки за середовищем ігор

Аспект захисту	Онлайн-ігри	Офлайн-ігри
Основні загрози	DDoS-атаки, фішинг, витоки даних, читери	Піратство, шкідливе ПЗ в модифікаціях, локальні експлойти
Ключові методи	MFA, firewalls, AI-моніторинг трафіку, шифрування даних	DRM-системи, хеш-перевірки файлів, антивірусні сканери
Рівень складності	Високий (мережевий, реального часу)	Середній (локальний, статичний)
Ефективність	Залежить від серверної інфраструктури, висока при інтеграції з хмарою	Висока для запобігання копіюванню, але нижча проти користувацьких помилок

Аналізуючи ефективність методів, в онлайн-іграх серйозні ігри для навчання кібербезпеки, такі як симуляції хакерських атак, показують високу залученість гравців, дозволяючи практикувати захист у віртуальному середовищі без реальних ризиків. Ці методи включають гейміфікацію, де елементи, як бали за правильні дії, мотивують до вивчення концепцій шифрування чи мереж. У офлайн-іграх подібні підходи рідкісні, але можуть проявлятися в освітніх модулях, інтегрованих у гру, для навчання базовим принципам безпеки. Порівняння демонструє, що онлайн-методи більш інтерактивні та адаптивні, тоді як офлайн фокусуються на статичному захисті. Актуальні огляди підкреслюють, що інтеграція гейміфікації підвищує ефективність навчання в обох типах, зменшуючи людський фактор як слабку ланку [5].

Розглядаючи еволюцію методів, в онлайн-іграх все частіше застосовуються AI-системи для виявлення аномальної поведінки, такі як автоматизовані боти чи читери, що аналізують патерни дій гравців у реальному часі. Це контрастує з офлайн, де AI може використовуватися для локальної перевірки файлів, але без мережевого компоненту. Порівняльні дослідження показують, що онлайн-ігри вимагають більш ресурсоємних методів через глобальну взаємодію, тоді як офлайн дозволяють економію ресурсів за рахунок локалізації. Однак у гібридних моделях, як у іграх з опціональним онлайн, методи комбінуються, забезпечуючи гнучкість. Це підкреслює тенденцію до уніфікації підходів для підвищення загальної безпеки індустрії [6].

У висновковій частині аналізу варто зазначити, що порівняльний підхід до методів кібербезпеки в онлайн та офлайн іграх розкриває необхідність балансу між технологічними інноваціями та освітою користувачів, аби мінімізувати ризики в еволюціонуючій цифровій екосистемі.

Список використаних джерел

1. Leder M., Sharadin G. Why Attackers Target the Gaming Industry. Imperva. URL: https://www.imperva.com/blog/cyber-attacks-gaming-industry/ (дата звернення: 30.10.2025).
2. The 10 biggest online gaming risks and how to avoid them. Kaspersky Lab. URL: https://www.kaspersky.com/resource-center/threats/top-10-online-gaming-risks (дата звернення: 30.10.2025).
3. Chattopadhyay S., Tiwari M., Tiwari T., Kapila D. Role of Cyber security in Gaming technology. 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). 2023. PP. 446-451. DOI: 10.1109/ICACITE57410.2023.10182589
4. Nanjundan P., Chinnasami S., Saravanan V., Ramachandran M. Contrasting the impact of online games and offline games: A comparative analysis. Contemporaneity of English Language and Literature in the Robotized Millennium. 2024. №2(4). PP. 28-36. DOI: 10.46632/cellrm/2/4/4
5. Coenraad M., et al. Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. Simulation & Gaming. 2024. №51(5). PP. 586-611. DOI: https://doi.org/10.1177/1046878120933312
6. Ng C. Y., Hasan M. K. B. Cybersecurity serious games development: A systematic review. Computers & Security. 2025. №150. DOI: https://doi.org/10.1016/j.cose.2024.104307

Ключові слова: кібербезпека, онлайн-ігри, офлайн-ігри, DDoS-атаки, фішинг, витоки даних, багатофакторна аутентифікація, цифрове управління правами, шифрування даних, AI-моніторинг, піратство, шкідливе програмне забезпечення.
Keywords: cybersecurity, online games, offline games, DDoS attacks, phishing, data leaks, multi-factor authentication, digital rights management, data encryption, AI monitoring, piracy, malware.

СИСТЕМА ВИЯВЛЕННЯ ВИТОКІВ ПЕРСОНАЛЬНИХ ДАНИХ

Бойко Віктор

кандидат технічних наук, доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Вередін Діана

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Зростання цифровізації суспільства призвело до підвищення цінності персональних даних, як активів. Використання інформаційних технологій, хмарних сервісів та віддаленого доступу до даних створює нові ризики та

загрози кібербезпеки. Наразі інформація про особистість, фінансові дані, медичні записи, контактні дані та багато іншої конфіденційної інформації зберігається, обробляється та циркулює в електронному вигляді, що стало причиною збільшення таких кіберінцидентів як витоки персональних даних.

Витік даних – це несанкціоноване розголошення делікатної, конфіденційної або особистої інформації із систем або мереж організації зовнішній стороні, що може бути навмисним або випадковим [1].

У зв'язку з зростаючою кількістю кібератак та масштабними витоками персональної інформації, питання її захисту набуває особливої актуальності. Використання лише таких заходів, як запобігання витоків даних (DLP) є недостатнім, оскільки будь-яка захисна інфраструктура компанії не гарантує абсолютну стійкість до сучасних загроз та безпеку зберігання та передачі чутливих чи конфіденційних даних. Згідно з звітністю International Business Machines Corporation (IBM), залежно від галуззі організації, для виявлення факту витоку інформації може знадобитись близько двохсот днів, а для локалізації та усунення наслідків ще близько шістдесяти днів [3]. На відміну від DPL-систем, що створені для запобігання витокам інформації у внутрішній мережі, використання автоматизованих систем виявлення скомпроментованих даних надає можливість розширити зону захисту за межі інфраструктури організації та забезпечити проактивну ідентифікацію ризиків. Швидкість виявлення витоку є головним фактором для мінімізації його наслідків, а завдяки процесу моніторингу та сповіщення про такі кіберінциденти, час між фактичним моментом витоку та його виявленням і реагуванням значно скорочується.

Персональні дані, що було викрадено внаслідок кібератак, часто поширюються через відкриті та закриті канали. Серед відкритих джерел зловмисники використовують пастбіни. Pastebin'и – це веб-сайти, де користувачі можуть зберігати онлайн великі обсяги тексту для зручного обміну, одним з таких сайтів є Pastebin.com [4]. Великі обсяги скомпроментованих даних циркулюють у закритих джерелах, до яких належать різні форуми, приватні канали, месенджери та сайти, що працюють в мережі Tor (The Onion Router). Доступ до таких джерел вимагає наявності спеціальних інструментів або знань. Існують сервіси, що надають можливість відслідковування факту витоку персональних даних в ручному режимі, Have I Been Pwned (HIBP) це один з таких сервісів. Він має велику базу даних, що містить записи про мільярди скомпроментованих облікових записів і постійно оновлюється [2].

Для забезпечення швидкості виявлення нових витоків персональних даних автоматизована система має використовувати гібридний підхід, що буде поєднувати використання вже готових баз даних з інформацією про великі відомі інциденти, як у сервісу HIBP, та власний автоматизований

механізм розрахований на виявлення нових, невеликих витоків у не очевидних джерелах. У таких сервісах як Pastebin та HIBP є власні API, що допоможуть зручно реалізувати автоматизовану систему виявлення, не перенавантажуючи необхідні сервіси. Після виявлення скомпроментованих даних співробітника, система негайно надсилає сповіщення про факт настання інциденту, деталі про джерело витоку, дані що було злито та інструкцію реагування на нього адміністратору системи безпеки.

Такий підхід до реалізації системи виявлення витоків конфіденційної інформації забезпечує захист даних за межами корпоративної мережі, гарантує швидке реагування, що зменшує фінансові та репутаційні втрати, сприяє покращенню обізнаності співробітників про загрози витоків їх персональних даних.

Список використаних джерел:

1. Що таке витік даних?| Захисний комплекс Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-data-leak.
2. Have I Been Pwned: Check if your email address has been exposed in a data breach. Have I Been Pwned. URL: https://haveibeenpwned.com.
3. IBM. URL: https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91.
4. Pastebin.com - FAQ [Frequently Asked Questions]. Pastebin. URL: https://pastebin.com/faq.

Ключові слова: витік персональних даних, система виявлення, кібербезпека, конфіденційна інформація, запобігання витокам даних (DLP), моніторинг, пастбін.
Keywords: personal data leak, detection system, cybersecurity, confidential information, Data Loss Prevention (DLP), monitoring, pastebin.

РОЗРОБКА ІНСТРУМЕНТУ АНАЛІЗУ ТА ОЦІНКИ БЕЗПЕКИ WI-FI МЕРЕЖ В УМОВАХ СУЧАСНИХ КІБЕРЗАГРОЗ

Бабенко Кирило

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасне інформаційне суспільство характеризується активним зростанням кількості мобільних пристроїв і широким упровадженням технологій Інтернету речей (IoT), що призвело до стрімкого збільшення залежності користувачів і організацій від бездротових мереж. Wi-Fi залишається однією з найпоширеніших технологій бездротового доступу до мережі Інтернет, проте водночас є одним із найуразливіших елементів інформаційно-комунікаційної інфраструктури [1]. Значна кількість Wi-Fi мереж і досі використовує слабкі паролі або застарілі протоколи шифрування (WEP, WPA), що робить їх вразливими до атак перебором паролів (bruteforce). За

даними аналітичних звітів ENISA Threat Landscape 2024, до 30 % інцидентів кібербезпеки в Європі пов'язані саме з уразливостями у конфігурації Wi-Fi мереж і відсутністю належного контролю доступу [5].

Однією з основних проблем забезпечення безпеки бездротових мереж є складність централізованого моніторингу, а також відсутність ефективних програмних рішень, які б дозволяли комплексно оцінювати стан захисту мережі. Традиційні засоби, такі як Aircrack-ng, Wifite або Kismet, хоча й мають потужний функціонал, орієнтовані переважно на досвідчених користувачів і не забезпечують інтегрованого підходу до аналізу вразливостей та автоматизації процесу тестування [2].

Вирішення цієї проблеми стало метою створення програмного комплексу «Babenko Wi-Fi», який поєднує інструменти моніторингу, тестування на проникнення, аналізу конфігурацій та формування рекомендацій у єдиному інтерфейсі.

Розроблений комплекс реалізовано мовою програмування Python, що забезпечує кросплатформеність і простоту інтеграції з існуючими системами тестування безпеки. Для створення графічного інтерфейсу використано бібліотеку Tkinter, яка дозволяє розробляти легкі та зрозумілі GUI-додатки. Для роботи з мережевими пакетами застосовано бібліотеку Scapy, яка підтримує створення, відправлення, перехоплення та аналіз будь-яких типів фреймів бездротових мереж [4]. Також реалізовано взаємодію з інструментами Aircrack-ng, що забезпечують перехоплення handshake-пакетів і перевірку стійкості паролів [3]. Модульна архітектура комплексу забезпечує гнучкість, масштабованість і можливість розширення функціоналу в майбутньому.

Комплекс «Babenko Wi-Fi» складається з п'яти основних модулів: сканування, перехоплення, підбору паролів, аналітики безпеки та логування результатів. Модуль сканування виконує виявлення всіх доступних Wi-Fi мереж у зоні дії пристрою та аналізує їхні характеристики (SSID, BSSID, RSSI, тип шифрування, наявність WPS). Модуль перехоплення handshake реалізує фіксацію чотиристороннього процесу автентифікації клієнта з точкою доступу, що є необхідним для подальшого аналізу або підбору паролів. Модуль підбору паролів реалізує словникові та маскові атаки з багатопотоковою обробкою, що дозволяє значно прискорити процес. Аналітичний модуль оцінює отримані результати, визначаючи стійкість пароля на основі його довжини, складності та ентропії, а також виявляє небезпечні параметри конфігурації (активний WPS, трансляція SSID, відсутність фільтрації MAC-адрес тощо). Модуль звітності зберігає результати тестування в базі даних і формує підсумкові звіти, що дозволяє використовувати комплекс у регулярному аудиті безпеки Wi-Fi мереж.

Під час експериментального тестування комплексу, проведеного у контрольованому середовищі, результати показали, що система успішно ідентифікує вразливі конфігурації, перехоплює handshake-пакети та проводить підбір паролів до слабозахищених мереж. Мережі з довгими складними паролями (понад 12 символів) та сучасними протоколами WPA3 залишилися стійкими до brute-force атак, що відповідає рекомендаціям NIST SP 800-153 [1].

Розробка має значну практичну цінність. Зокрема, програмний комплекс «Babenko Wi-Fi» може використовуватись як інструмент для внутрішнього аудиту безпеки в організаціях, допомагаючи виявляти слабкі місця до їхньої експлуатації зловмисниками. Крім того, система може бути ефективно застосована в освітньому процесі під час підготовки студентів і фахівців з кібербезпеки, оскільки забезпечує практичне розуміння принципів шифрування, автентифікації та виявлення вразливостей. Також програмний комплекс дозволяє проводити оцінку ефективності вже впроваджених заходів безпеки, що важливо для підтримки високого рівня кіберстійкості інформаційно-комунікаційних систем.

Розроблений інструмент є внеском у розвиток практичних засобів кіберзахисту, оскільки забезпечує комплексну оцінку безпеки Wi-Fi мереж, підвищує рівень кіберстійкості інформаційних систем і сприяє формуванню сучасної культури інформаційної безпеки серед користувачів і спеціалістів галузі.

Список використаних джерел:

1. National Institute of Standards and Technology (NIST). Guidelines for Securing Wireless Local Area Networks (WLANs). NIST SP 800-153, Gaithersburg, MD, 2012. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf
2. OWASP Foundation. *Wi-Fi Security Testing Guide.* OWASP Project, 2024. URL: https://owasp.org/www-project-wifi-testing-guide/
3. Aircrack-ng Project. *Aircrack-ng – Wi-Fi Security Auditing Tools.* Official Documentation, 2024. URL: https://www.aircrack-ng.org/
4. Scapy Community. Scapy Documentation: Packet Manipulation in Python. ReadTheDocs, 2024. URL: https://scapy.net/
5. ENISA. *ENISA Threat Landscape 2024.* European Union Agency for Cybersecurity, 2024. URL: https://www.enisa.europa.eu/topics/threat-landscape

Ключові слова: кібербезпека, Wi-Fi мережі, тестування на проникнення, аналіз вразливостей, handshake, bruteforce, оцінка безпеки, програмний комплекс.
Keywords: cybersecurity, Wi-Fi networks, penetration testing, vulnerability analysis, handshake, bruteforce, security assessment, software complex.

ГЕНЕРАЦІЯ ДИНАМІЧНИХ S-БЛОКІВ (F-БЛОКІВ) НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

Роговий Іван

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

S-блоки є фундаментальним компонентом симетричних криптографічних алгоритмів, від властивостей яких безпосередньо залежить стійкість шифрів до диференціального та лінійного криптоаналізу. Використання статичних S-блоків у режимах довготривалої експлуатації супроводжується низкою обмежень, оскільки накопичення статистичної інформації та застосування адаптивних атак можуть призводити до зниження рівня криптографічного захисту. У цьому контексті особливий інтерес становлять динамічні S-блоки (F-блоки), структура яких змінюється в процесі функціонування алгоритму. Такий підхід ускладнює накопичення релевантної статистики для криптоаналізу та сприяє підвищенню загальної криптостійкості симетричних криптосистем.

Метою роботи є аналіз і обґрунтування ідеї використання еліптичних кривих для генерації динамічних S-блоків (F-блоків), а також оцінка криптографічних властивостей і перспектив застосування такого підходу в симетричних криптографічних алгоритмах.

S-блоки (substitution boxes) є ключовими нелінійними перетвореннями симетричних криптографічних алгоритмів, призначеними для забезпечення конфузії (confusion) між відкритим текстом, ключем і шифротекстом. Вони реалізують відображення вхідних бітових векторів у вихідні, формуючи основне джерело нелінійності в структурі шифру. Саме властивості S-блоків значною мірою визначають криптографічну стійкість алгоритмів до основних видів статистичного криптоаналізу, зокрема диференціального та лінійного.

До основних криптографічних характеристик S-блоків належать висока нелінійність, низька диференційна однорідність, збалансованість, відсутність фіксованих точок і лінійних апроксимацій із великою ймовірністю. Порушення цих вимог призводить до зниження стійкості шифру та створює передумови для ефективних атак. У зв’язку з цим розроблення та аналіз S-блоків із покращеними характеристиками є однією з центральних задач сучасної симетричної криптографії.

F-блоки реалізують динамічну зміну таблиці замін залежно від параметрів криптографічної сесії, секретного ключа або внутрішнього стану алгоритму, що суттєво знижує ефективність атак, заснованих на накопиченні статистичної інформації для фіксованих S-блоків. Формування таких таблиць може здійснюватися детерміністичним способом на основі ключа або початкового значення, із застосуванням генераторів псевдовипадкових

послідовностей, хаотичних відображень чи інших математичних конструкцій. Окремий інтерес становлять підходи, що використовують математичний апарат еліптичних кривих [1], у яких координати точок та результати групових операцій слугують джерелом високої ентропії для побудови перестановок. Застосування еліптичних кривих дозволяє поєднати високу криптографічну міцність із детерміністичною відтворюваністю структури F-блоку за наявності коректного ключа, що є принципово важливим для практичної реалізації симетричних криптосистем.

Алгоритм генерації F-блоків має задовольняти низку принципових вимог. Зокрема, він повинен гарантувати бієктивність відображення, тобто формування коректної перестановки значень, а також забезпечувати високий рівень нелінійності та низькі значення диференціальних і лінійних характеристик. Важливою практичною умовою є прийнятна обчислювальна складність і швидкість генерації, що визначає можливість реального впровадження алгоритму в симетричних криптосистемах. Крім того, алгоритм має бути стійким до відновлення структури F-блоку на основі часткових спостережень або побічної інформації, що є критичним для забезпечення довготривалої криптографічної безпеки. Для ілюстрації запропонованого підходу розглянемо узагальнену концептуальну схему формування динамічних S-блоків (F-блоків) із використанням операцій над еліптичними кривими. Наведена схема має ілюстративний характер і демонструє принципову можливість практичної реалізації ідеї, не претендуючи на завершену криптографічну специфікацію.

Орієнтовна схема генерації F-блоку може включати такі етапи:

1. В якості вхідних параметрів використовується симетричний ключ K та внутрішній сід S, який може формуватися як функція від ключа та випадкового вектора.
2. На основі пари $\{K,S\}$ генерується послідовність скалярів k_i, що визначають подальші операції на еліптичній кривій.
3. Для кожного значення k_i може обчислюватися відповідна точка $P_i = k_i G$ на еліптичній кривій, де G – фіксована базова точка.
4. Координати (x_i, y_i) отриманих точок перетворюються у бітові послідовності, які можуть використовуватися як джерело псевдовипадкових даних для побудови перестановки, зокрема із застосуванням алгоритму Фішера-Йетса.
5. Результатом є бієктивна перестановка значень (наприклад, множини $0...255$ для 8-бітного S-блоку), що визначає таблицю замін F-блоку.

Використання процедур перетасування гарантує бієктивність сформованого S-блоку за умови коректного контролю повторів у псевдовипадковій послідовності. У практичних реалізаціях це може

досягатися шляхом відкидання некоректних значень або повторної ініціалізації сіду.

Запропонована концептуальна схема демонструє, що операції над еліптичними кривими можуть бути ефективно використані як джерело керованої псевдовипадковості для формування динамічних S-блоків із детермінованою відтворюваністю за наявності ключа.

Побудовані S-блоки (F-блоки) підлягають обов'язковому тестуванню на відповідність базовим критеріям криптографічної якості [2], що дозволяють оцінити їхню придатність для використання в симетричних криптосистемах. До таких критеріїв належать алгебраїчна нелінійність, відстань нелінійності, диференціальна та лінійна стійкість, лавинні й кореляційні властивості. Оцінювання зазначених характеристик є необхідним для підтвердження здатності F-блоків протидіяти основним видам статистичного криптоаналізу.

Нелінійність S-блоків визначається як мінімальна відстань Хеммінга між булевими функціями, що утворюють S-блок, та множиною всіх афінних функцій. Використання послідовностей, сформованих на основі операцій над точками еліптичних кривих, дозволяє очікувати високі значення нелінійності завдяки їхній структурній непередбачуваності. Диференціальна стійкість аналізується за допомогою матриці диференціальних переходів (DDT), причому динамічний характер F-блоків призводить до розмивання статистичних залежностей між сесіями, що знижує ймовірність виявлення корисних диференціальних відмінностей.

Лавинні властивості оцінюються шляхом аналізу впливу малих змін ключа або початкового значення на структуру F-блоку, що має спричиняти суттєву реконфігурацію таблиці замін та забезпечувати як локальну, так і глобальну дифузію. Додатково аналізуються кореляційні характеристики шляхом дослідження лінійних апроксимацій, зокрема із застосуванням лінійної апроксимаційної матриці.

Методика тестування передбачає генерацію множини F-блоків для різних значень початкових параметрів, подальше обчислення їхніх криптографічних характеристик, аналіз лавинного ефекту на входах і виходах, а також дослідження поведінки F-блоків за умов часткової відомості відкритого тексту. Для розширеного аналізу можливе застосування апарату багатозначної логіки, який дозволяє узагальнено оцінювати нелінійні та кореляційні властивості криптографічних конструкцій у ширшому алгебраїчному просторі.

Питання продуктивності та оптимізації є принципово важливими для практичного застосування F-блоків, побудованих на основі еліптичних кривих. Генерація таких блоків передбачає виконання операцій множення точки на скаляр, які є обчислювально затратними порівняно з традиційними табличними S-блоками. З метою зменшення обчислювальних витрат можливе

застосування попереднього кешування F-блоків на етапі ініціалізації криптографічної сесії, використання ефективних представлень еліптичних кривих (зокрема форм Монтгомері або Едвардса), а також апаратне прискорення з використанням спеціалізованих процесорів, FPGA або ASIC. Додатковим шляхом оптимізації є обмеження частоти реконфігурації F-блоку, наприклад, на рівні сесії, а не кожного блоку повідомлення. Таким чином, ключовим завданням є балансування між частотою оновлення F-блоку та витратами обчислювальних ресурсів і пам'яті. Коректний вибір інтервалу оновлення дозволяє досягти необхідного рівня криптографічної безпеки без критичного зниження продуктивності системи, що є особливо важливим для вбудованих та високонавантажених середовищ.

Висновки та практичні рекомендації. Дослідження показує, що динамічні S-блоки на основі еліптичних кривих представляють перспективний напрямок підвищення криптостійкості симетричних шифрів, оскільки їхня зміна в процесі роботи суттєво ускладнює збір корисної статистики про заміни. Критично важливо, щоб алгоритм генерації забезпечував бієктивність та високий рівень нелінійності, що потребує обов'язкового емпіричного тестування на відповідність основним криптографічним критеріям при кожній реалізації. Для практичного застосування слід оптимізувати процес генерації F-блоків, використовуючи кешування, ефективні представлення еліптичних кривих та апаратне прискорення, а також передбачити заходи захисту від атак по сторонніх каналах. Рекомендується інтегрувати F-блоки у комплексну криптографічну стратегію, поєднуючи динамічні блоки, надійні схеми управління ключами та політики їх ротації, що забезпечує високий рівень захисту та практичну придатність симетричних систем шифрування.

Список використаної літератури:

1. Alali A.S. et al. Dynamic S-Box Construction Using Mordell Elliptic Curves over Galois Field and Its Applications in Image Encryption. Mathematics, 2024. 12(4). P. 587
2. Karpinski M., Sokolov A., Tokkuliyeva A., Radush V., Kazakova N., Shaikhanova A., Zagorodna N., Korchenko A. Development of High-Quality Cryptographic Constructions Based on Many-Valued Logic Affine Transformations. Electronics. 2025. Vol. 14, Issue 10. P. 1-22.

Ключові слова: F-блоки, динамічні S-блоки, симетричні шифри, криптостійкість, диференціальний та лінійний криптоаналіз, еліптичні криві, нелінійність, лавинні властивості, багатозначна логіка.
Keywords: F-boxes, dynamic S-boxes, symmetric ciphers, cryptoresistance, differential and linear cryptanalysis, elliptic curves, nonlinearity, avalanche properties, many-valued logic.

СТВОРЕННЯ ФІШИНГОВОГО СЦЕНАРІЮ ТА АНАЛІЗ РЕАКЦІЇ КОРИСТУВАЧІВ

Тинкевич Дана

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Фішинг залишається однією з найпоширеніших і найрезультативніших форм кібератак, спрямованих на компрометацію конфіденційних даних користувачів і організацій. Сучасні фішингові повідомлення та вебсторінки дедалі точніше імітують легітимні сервіси, використовуючи знання про поведінкові особливості та емоційні тригери людини. Попри розвиток технічних засобів захисту, ефективність протидії фішингу значною мірою обмежується людським фактором. У цьому контексті навчальні фішингові симуляції є важливим інструментом для виявлення реальних поведінкових вразливостей і формування практичних навичок кібергігієни.

Незважаючи на значну кількість публікацій, присвячених технічним аспектам виявлення та блокування фішингових атак, значно менш дослідженим залишається поведінковий аспект взаємодії користувачів із фішинговими ресурсами, зокрема в умовах, наближених до реальних. Більшість наявних робіт зосереджується на автоматизованих методах захисту, тоді як емпіричні дослідження реакції користувачів у контрольованих навчальних симуляціях є обмеженими. Це ускладнює формування практично орієнтованих рекомендацій, спрямованих на зниження впливу людського фактора в системах інформаційної безпеки.

Метою даної роботи є розроблення навчального фішингового сценарію та дослідження на його основі поведінки користувачів під час взаємодії з підробною сторінкою автентифікації, з подальшою оцінкою чинників, що впливають на успішність атаки, та формуванням практичних рекомендацій щодо підвищення рівня захисту від фішингових загроз.

Фішинг – це форма соціальної інженерії, коли зловмисник під виглядом легітимного сервісу або особи змушує жертву розкрити конфіденційні дані (логіни, паролі, платіжні реквізити) або виконати небезпечну дію (завантажити шкідливий файл, перейти за посиланням) [1].

Фішингові атаки можуть бути класифіковані за цілями та каналами реалізації. Зокрема, класичний (масовий) фішинг передбачає розсилання великої кількості електронних листів або повідомлень із посиланнями на підроблені ресурси. Цільовий фішинг (spear-phishing) спрямований на конкретну особу або роль та використовує персоналізовану інформацію про жертву. Окремим різновидом є whaling, що орієнтований на керівників і посадових осіб високого рівня. Залежно від каналу комунікації виділяють smishing та vishing, які реалізуються відповідно через SMS-повідомлення та

голосові дзвінки. Крім того, pharming базується на перенаправленні користувачів на фальшиві вебресурси на рівні DNS або шляхом компрометації мережевої інфраструктури, тоді як clone phishing полягає у створенні копії легітимного повідомлення з підміною гіперпосилання на фішингове [2].

Фішингова атака зазвичай реалізується не як одноразова дія, а як послідовний багатоетапний процес, у межах якого зловмисник поєднує технічні та соціально-інженерні прийоми. Аналіз структури фішингових кампаній дозволяє виокремити ключові етапи, кожен з яких відіграє окрему роль у досягненні кінцевої мети:

1. *Розвідка* – збір публічної інформації про ціль (профілі, контакти, корпоративна структура).
2. *Створення приманки* – дизайн листа/сторінки, імітація бренду (логотипи, стилістика, мова).
3. *Доставка* – вибір каналу (email, месенджери, соцмережі, SMS).
4. *Захоплення даних* – сторінки введення, форми, скрипти для логування.
5. *Використання* – доступ до акаунтів, фінансові операції, ескалація атак.

Ефективність фішингових атак значною мірою зумовлена використанням психологічних механізмів впливу на користувачів. Застосування відчуття терміновості, апеляція до страху втрати (наприклад, можливого блокування облікового запису), обіцянка потенційної вигоди, імітація авторитетного джерела, а також персоналізація повідомлень у сукупності знижують рівень критичного сприйняття інформації та істотно підвищують імовірність введення конфіденційних даних користувачем.

Для досягнення поставленої мети було розроблено навчальний фішинговий сценарій, реалізований у вигляді контрольованої технічної симуляції. Технічна частина дослідження спрямовувалася на відтворення типових елементів фішингової атаки в безпечному ізольованому середовищі з дотриманням етичних вимог та мінімізацією потенційних ризиків для учасників експерименту:

- Застосовано ізольовану тестову інфраструктуру (локальний сервер на LAMP/LEMP) для безпечного проведення експерименту.
- Створено HTML/CSS/JS-шаблон, що імітує сторінку входу популярного сервісу, без викликів до реальних доменів.
- Серверна частина (Python/Flask) забезпечувала логування анонімізованих введень у файл або базу даних; дані шифрувалися і не зберігалися довгостроково.

- Після введення користувачу показувалось нейтральне повідомлення або перенаправлення, щоб не викликати додаткових підозр.
- Дотримано етичних обмежень: участь тільки за письмовою згодою, відсутність збору реальних паролів від робочих систем, подальше інформування учасників та навчальні матеріали після завершення.

У межах експериментального сценарію учасникам, об'єднаним у закриту навчальну групу, надсилалося повідомлення з пропозицією виконати дію, що імітувала типову фішингову комунікацію (наприклад, перевірити обліковий запис або отримати результат). Повідомлення містило посилання на підробну сторінку автентифікації, на якій користувачам пропонувалося ввести логін і пароль. Усі введені дані фіксувалися в анонімізованому вигляді виключно з дослідницькою метою. Після завершення експерименту учасники отримували роз'яснення щодо характеру проведеної симуляції та навчальні матеріали з основ кібергігієни.

Для оцінювання результатів експерименту було сформовано систему кількісних і якісних показників, що характеризують поведінкові реакції користувачів під час взаємодії з навчальним фішинговим сценарієм. Узагальнення отриманих даних засвідчило наявність стійких поведінкових патернів, пов'язаних із реагуванням на фішингові стимули. Зокрема, було зафіксовано переходи за фішинговим посиланням та введення облікових даних без попередньої перевірки доменного імені або параметрів безпеки з'єднання, тоді як випадки звернення уваги на потенційно підозрілі ознаки ресурсу мали поодинокий характер. Аналіз часових характеристик взаємодії, відмов від введення даних і звернень за допомогою свідчить про те, що застосування базових соціально-інженерних тригерів, зокрема терміновості та апеляції до авторитету, позитивно корелює з ефективністю навіть технічно простих імітацій інтерфейсу.

Висновки. У ході дослідження було продемонстровано, що ефективність фішингових атак значною мірою визначається не технічною складністю підробки, а якістю соціально-інженерного впливу. Отримані результати свідчать про те, що правильно сформульована легенда, використання психологічних тригерів і форма комунікації здатні забезпечувати високу результативність навіть за умови спрощеної візуальної імітації інтерфейсу.

Аналіз поведінкових реакцій користувачів підтвердив домінуючу роль людського фактора в сучасних загрозах фішингу. Це зумовлює необхідність поєднання технічних засобів захисту, зокрема двофакторної автентифікації, антифішингових фільтрів, механізмів захищеного DNS і контролю сертифікатів, із системними організаційними та освітніми заходами. Регулярні тренінги, контрольовані симуляції фішингових атак і формування культури

інформаційної безпеки істотно підвищують здатність користувачів розпізнавати загрози та коректно реагувати на інциденти.

Окрему увагу в роботі приділено етичним і правовим аспектам проведення навчальних фішингових симуляцій. Показано, що подібні дослідження є допустимими виключно за умов інформованої згоди учасників, мінімізації потенційної шкоди, прозорості методики та обов'язкового видалення чутливих даних після завершення аналізу.

Практична значущість отриманих результатів полягає в можливості їх застосування під час розроблення програм підвищення обізнаності з кібербезпеки, створення внутрішніх регламентів реагування на фішингові інциденти та впровадження обов'язкових механізмів багатофакторного захисту в освітніх і корпоративних інформаційних системах.

Список використаної літератури:

1. Putra F. P. E. et al. Analysis of phishing attack trends, impacts and prevention methods: literature study. Brilliance: Research of Artificial Intelligence. 2024. Vol. 4, No. 1. P. 413-421.
2. Alghenaim M. F. et al. Phishing attack types and mitigation: A survey. The International Conference on Data Science and Emerging Technologies. Singapore : Springer Nature Singapore, 2022. P. 131-153.

Ключові слова: фішинг, фішингова атака, поведінкові вразливості, людський фактор, соціальна інженерія, навчальна фішингова симуляція, кібергігієна, аналіз реакції користувачів, кібербезпека.
Keywords: phishing, phishing attack, behavioral vulnerabilities, human factor, social engineering, educational phishing simulation, cyber hygiene, user reaction analysis, cybersecurity.

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАХИСТУ ЛОГІВ

Бойко Віктор

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат технічних наук

Вуль Анастасія

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасні інформаційно-комунікаційні системи (ІКС) генерують величезні обсяги логів – журналів подій, що є основним джерелом інформації для моніторингу, виявлення інцидентів безпеки та розслідування кібератак [1]. Саме на основі логів фахівці з кібербезпеки визначають, коли і як відбулося

вторгнення, встановлюють причини інцидентів та відновлюють хронологію подій. Проте традиційні системи зберігання логів виявляються вразливими до фальсифікацій, несанкціонованих змін та видалення даних [2]. Зловмисник, отримавши доступ до серверів, може не лише здійснити атаку, а й приховати свої сліди шляхом модифікації логів. Це унеможливлює об'єктивне розслідування події та значно знижує довіру до систем кіберзахисту, навіть у доброчесних адміністраторів виникає проблема довіри до даних логів, адже вони зберігаються централізовано і не мають захисту від внутрішнього втручання.

Проблема автентичності та цілісності логів стає критичною у контексті сучасних кібератак, особливо для великих корпорацій, державних установ і провайдерів послуг. Одним із найперспективніших напрямів вирішення цієї проблеми є застосування технології блокчейн для децентралізованого зберігання логів [3]. Використання блокчейну дозволяє створити незмінну хронологічну послідовність записів, де кожен блок є криптографічно захищеним і пов'язаний із попереднім. Це унеможливлює підробку чи знищення записів навіть у разі компрометації окремих вузлів системи [4].

Тому постає питання: як зробити логи незмінними, достовірними та перевірюваними? Відповіддю може бути використання технології блокчейн, яка дозволяє створювати децентралізовану, прозору й захищену систему зберігання логів.

Мета даного дослідження – розробити концепцію системи виявлення вторгнень, у якій усі журнали подій (логи) записуються до блокчейну, що забезпечує їхню цілісність, автентичність і неможливість фальсифікації.

Система зберігання логів на базі блокчейну необхідна:

- організаціям із підвищеними вимогами до кіберзахисту, де важливо мати достовірні докази у випадку інцидентів (банки, держустанови, енергетичні компанії);
- хмарним провайдерам та дата-центрам, які обробляють великі обсяги журналів із різних серверів і клієнтів;
- командам безпеки (SOC), що проводять моніторинг, аудит і реагування на інциденти;
- системам штучного інтелекту для кіберзахисту, яким потрібні достовірні навчальні дані з реальних логів.

Для всіх цих випадків ключовою вимогою є довіра до логів: якщо дані можуть бути підроблені, уся система аналітики втрачає сенс.

Система виявлення вторгнень із блокчейн-захистом логів поєднує класичні механізми збору подій із децентралізованим зберіганням.

Основні етапи роботи виглядають так:

1. Збір логів. Модулі-агенти встановлюються на вузлах мережі (сервери, маршрутизатори, робочі станції). Вони відстежують події авторизації, мережевий трафік, помилки системи, запити до баз даних тощо.

2. Формування запису. Кожен лог перетворюється на структурований об'єкт, що містить часову мітку, джерело події, тип активності, цифровий підпис агента.

3. Хешування та запис у блокчейн. Система обчислює SHA-512 хеш від змісту запису та додає його у блок разом із попереднім хешем. Завдяки цьому будь-яка спроба змінити лог змінить увесь ланцюг блоків.

4. Розповсюдження між вузлами. Копія блокчейну зберігається на кількох вузлах системи. Навіть якщо один сервер буде зламаний, дані можна перевірити через інші копії.

5. Виявлення вторгнень. Аналітичний модуль аналізує нові логи (зокрема з використанням машинного навчання або сигнатур), фіксує підозрілі дії й створює відповідний блок у ланцюгу.

6. Верифікація логів. Адміністратор може будь-коли перевірити справжність записів, порівнявши хеші з блокчейну з локальними журналами.

Переваги підходу: Незмінність(жоден запис логу не може бути видалений або змінений без сліду), Децентралізація(логи не зберігаються на одному сервері — це унеможливлює знищення доказів атаки), прозорість(усі учасники системи мають однакову копію блокчейну, що гарантує єдиний стан журналів), доказовість(у разі розслідування кібератак логи з блокчейну можуть виступати надійними цифровими доказами), автоматизація(смарт-контракти можуть автоматично створювати сповіщення чи блокувати IP-адреси при повторних інцидентах).

Таким чином, система забезпечує не лише виявлення загроз, а й захист самих даних, на основі яких робиться аналіз.

У процесі дослідження було проведено аналіз сучасних систем управління логами (ELK Stack, Splunk, Graylog) та рішень із використанням блокчейн-технологій у сфері інформаційної безпеки [6]. Виявлено, що хоча вони забезпечують потужну аналітику, але не гарантують незмінність записів.

Для усунення цього недоліку було розроблено прототип гібридної системи, що об'єднує збір логів із блокчейн-зберіганням.

До складу прототипу входять:

- Агент збору логів на Python, який зчитує системні журнали подій і перетворює їх на транзакції.
- Модуль хешування для створення криптографічних відбитків (SHA-512).

- Приватний блокчейн на основі технології Hyperledger Fabric, який зберігає усі записи.
- Веб-інтерфейс для перегляду журналів, перевірки їх автентичності та моніторингу атак.

Тестування показало, що навіть при спробі вручну змінити лог на сервері, хеш перевірки не збігається з записом у блокчейні, і система фіксує факт підробки. Це доводить ефективність методу для гарантованої цілісності логів у корпоративних мережах.

У ході роботи ми довели, що використання технології блокчейн для зберігання логів у системах виявлення вторгнень дозволяє вирішити одразу кілька критичних проблем:

- забезпечити цілісність журналів подій;
- гарантувати достовірність даних навіть при зламі сервера;
- створити повну історію змін і часову хронологію подій.

Ми реалізували прототип, який успішно фіксує події безпеки, записує їх у блокчейн і дозволяє перевіряти справжність логів у будь-який момент. Система продемонструвала стабільність, масштабованість і повну відсутність можливостей для маніпуляцій із записами.

Ми змогли об'єднати аналітику безпеки з криптографічним захистом журналів, створивши інноваційний підхід до моніторингу інцидентів. Цей підхід не лише підвищує рівень довіри до систем виявлення вторгнень, а й формує нову культуру прозорого зберігання цифрових доказів.

Подальші кроки в розвитку проєкту передбачають:

- розширення системи для обробки великої кількості логів у реальному часі;
- застосування штучного інтелекту для аналізу шаблонів атак у блокчейні;
- інтеграцію з існуючими IDS, такими як Snort або Suricata;
- реалізацію розподіленої аналітики, коли різні організації можуть спільно перевіряти достовірність логів, не розкриваючи конфіденційних даних.

Таким чином, створена система є важливим кроком у розвитку прозорих, надійних і стійких до фальсифікації систем безпеки, у центрі яких стоїть захищений журнал подій — лог, гарантований технологією блокчейн.

Список використанних джерел:

1. Zyskind G., Nathan O., Pentland A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops, 2015. URL: https://ieeexplore.ieee.org/document/7163223
2. Conti M., Dehghantanha A., Franke K., Watson S. Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications. IEEE Communications Surveys & Tutorials, 2018. URL: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9739
3. Kshetri N. 1 Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. Telecommunications Policy, 2017. URL: https://www.sciencedirect.com/science/article/abs/pii/S0308596117302483
4. Бойко В., Василенко М., Слатвінська В. *Моделювання живучості та відновлення інформаційно-комунікаційних мереж в умовах дії кіберзагроз.* Інформаційні технології та суспільство, 2024, №1 (12), с. 13–19. URL: https://journals.maup.com.ua/index.php/it/article/view/3143
5. Lihua Song, Zongke Zhu, Menghen Li, Li Ma, Xinran Ju. A Novel Access Control for Internet of Things Based on Blockchain Smart Contract. IEEE Access, 2021. URL: https://ieeexplore.ieee.org/document/9390662
6. GDPR-Compliant Use of Blockchain for Secure Usage Logs – Zieglmeier V., Loyola Daiqui G, 2021. URL: https://arxiv.org/abs/2104.09971?utm_source=chatgpt.com

Ключові слова: блокчейн, журналювання, цілісність логів, система виявлення вторгнень, Hyperledger Fabric, SHA-512, цифрові докази, незмінність даних, криптографічний хеш-ланцюг.

Keywords: blockchain, logging, log integrity, intrusion detection system (IDS), Hyperledger Fabric, SHA-512, digital evidence, data immutability, cryptographic hash chain.

ПРОВЕДЕННЯ SQL-ІН'ЄКЦІЇ З ВИКОРИСТАННЯМ SQLMAP

Клевець Михайло

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

SQL-ін'єкції – одна з найстаріших та одночасно найефективніших технік компрометації вебзастосунків: при вдалому використанні вони дозволяють читати, змінювати або видаляти дані, отримувати облікові дані, а іноді й виконувати команди операційної системи.

Автоматизація атак (наприклад, із застосуванням SQLMap) значно знижує поріг входу для зловмисника і дозволяє за короткий час провести розвідку та екстракцію даних. Це робить регулярне тестування критично важливим для розробників і адміністраторів.

У даних тезах досліджуються методи проведення SQL-ін'єкцій та автоматизація таких атак із використанням утиліти SQLMap. З огляду на те,

що вебзастосунки широко використовують реляційні бази даних і SQL-запити, вразливості на рівні запитів залишаються критичною загрозою безпеці інформації.

Мета роботи – дослідити типи SQL-ін'єкцій, показати їх реалізацію у тестовому середовищі (DVWA), продемонструвати можливості SQLMap та розробити практичні заходи захисту.

У результаті проведеного дослідження узагальнено класифікацію систем керування базами даних (СКБД), зокрема реляційних, документних, ключ-значення, колонкових, графових і гібридних СКБД, та визначено їх характерні особливості з погляду безпеки. Встановлено, що реляційні СКБД (MySQL, PostgreSQL, MS SQL Server, Oracle, MariaDB, SQLite, IBM Db2) є найбільш поширеною основою сучасних вебзастосунків і водночас типовим середовищем виникнення SQL-уразливостей. На основі аналізу предметної області сформовано детальну класифікацію SQL-ін'єкцій, зокрема *in-band* (error-based, union-based), *blind* (boolean-based, time-based), *out-of-band*, *second-order* та NoSQL-ін'єкцій.

За результатами практичної частини підтверджено, що за наявності вразливих параметрів і відсутності належної обробки введених даних вебзастосунки з реляційною базою даних є вразливими до різних типів SQL-ін'єкцій, включаючи *blind* та *second-order* атаки. Експериментально встановлено можливість витягування структури бази даних і її вмісту (таблиць, стовпців і значень), що підтверджує критичний характер зазначених уразливостей у реальних сценаріях експлуатації.

У ході дослідження проаналізовано архітектуру та функціональні можливості інструмента SQLMap і встановлено його здатність автоматизовано виявляти SQL-уразливості з використанням різних технік (*boolean-based*, *time-based*, *union-based*, *error-based*, *stacked*, *out-of-band*), а також працювати з параметрами HTTP-запитів, cookie, заголовками та мережевими посередниками. Визначено набір ключових параметрів конфігурації SQLMap, застосування яких забезпечує гнучке керування процесом тестування та підвищує ефективність виявлення вразливостей.

Експериментальні результати підтвердили можливість автоматизованого отримання інформації про структуру бази даних (перелік баз даних, таблиць і стовпців), витягування вибраних даних, а також аналізу облікових даних, включно з отриманням і розпізнаванням хешів паролів у контрольованому середовищі. Окремо встановлено, що за наявності відповідних привілеїв SQLMap підтримує використання позасмугових каналів взаємодії та може забезпечувати виконання команд операційної системи.

В результаті вдалося підтвердити, що застосування автоматизованих інструментів істотно скорочує час розвідки та експлуатації SQL-уразливостей

порівняно з ручними методами, водночас підвищуючи повноту та відтворюваність результатів тестування.

Висновки. У результаті дослідження встановлено, що за відсутності захисних заходів SQL-ін'єкції дозволяють отримувати конфіденційні дані, порушувати цілісність та доступність інформації, а також здійснювати ескалацію привілеїв. Факторами, що підвищують ризик атак, є відсутність валідації та екранування введених даних, використання динамічних конкатенованих SQL-запитів, зайві права облікових записів баз даних, а також відсутність захисту на рівні мережі та журналювання. Обмеженням дослідження є те, що експерименти виконано у тестовому середовищі; результати є репрезентативними для подібних конфігурацій, проте у реальних системах фактори інфраструктури та політик доступу можуть впливати на прояви атак.

На основі отриманих результатів сформульовано рекомендації щодо захисту вебзастосунків, зокрема застосування параметризованих запитів (prepared statements) або ORM, валідацію та нормалізацію введених даних, обмеження прав облікових записів за принципом найменшого привілею, регулярне автоматизоване тестування з використанням таких інструментів, як SQLMap, а також впровадження систем виявлення вторгнень (IDS/IPS), логування та моніторинг аномалій у запитах. Доцільним є багаторівневий захист із використанням WAF, обмеженням частоти запитів та CAPTCHA на критичних формах.

Отримані рекомендації можуть бути безпосередньо впроваджені в процес розробки програмного забезпечення та політику інформаційної безпеки організації. Проведене дослідження підтверджує необхідність системного підходу до захисту вебзастосунків: поєднання безпечного коду, належного адміністрування баз даних та регулярного тестування є ключем до зниження ризиків, пов'язаних із SQL-ін'єкціями.

Список використаної літератури:

1. Nasereddin M. et al. A systematic review of detection and prevention techniques of SQL injection attacks. Information Security Journal: A Global Perspective. 2023. Vol. 32, No. 4. P. 252-265.
2. Subbulakshmi T. et al. SQL Injection Testing on Website using Sqlmap. International Conference on Trends in Quantum Computing and Emerging Business Technologies. IEEE, 2024. P. 1-4.

Ключові слова: SQL-ін'єкція, веб-безпека, реляційні бази даних, SQLMap, автоматизація атак, тестування вразливостей.
Keywords: SQL injection, web security, relational databases, SQLMap, attack automation, vulnerability testing.

СИСТЕМНИЙ АНАЛІЗ ТА ОЦІНКА РИЗИКІВ ВРАЗЛИВОСТІ IoT-ПРИСТРОЇВ

Гура Володимир

доцент, кандидат технічних наук, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Мурзін Олександр

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сьогодні в сучасному будинку є багато розумних пристроїв - камера на дверях, розумна розетка для чайника, колонка з голосовим помічником, термостат на батареї, робот-пилосос, розумні ваги, кавоварка, дитяча іграшка. За даними дослідження 2025 року, до кінця поточного року в Україні буде понад 50 мільйонів підключених IoT-пристроїв [1]. Це зручно, але небезпечно.

У 2024 році хакери зламали 1,5 мільйона розумних камер у Європі і транслювали відео у даркнет [2]. У 2023 році через вразливість у розумній розетці в одній з європейських квартир сталася пожежа – пристрій увімкнули віддалено на максимальну потужність [3]. У 2025 році було зламано 300 тисяч роботів-пилососів – вони знімали людей під час сну [4]. Дослідження в журналі Sensors 2024 року показало, що 70% домашніх IoT-пристроїв мають вразливості, які можна знайти за 10 хвилин [5].

Але більшість користувачів IoT-пристроїв уявлення не мають, як перевірити їх захищеність. Технічні терміни лякають, а виробники часто приховують проблеми у цьому напрямку. Тому слід звернути увагу на надання простого, зрозумілого і науково обґрунтованого способу перевірити на вразливість всі IoT-пристрої у розумному домі за короткий час, тоб-то розробити чек-лист, у якому буде надана методика, що базується на аналізі провіднх наукових досліджень.

Розумні камери часто стають першими жертвами через слабкі паролі, дослідження в IEEE Access 2023 року показало – 72% камер Tuya, Xiaomi, EZVIZ використовують пароль за замовчуванням типу admin або 12345678 [3], а в 2024 році в Applied Sciences зафіксовано – 41% камер передають відео без шифрування [6]. Розумні колонки Alexa, Google Home мають мікрофони, які можуть активуватися помилково; стаття в Frontiers in Big Data 2024 року зазначила – 28% пристроїв надсилають аудіо в пов‘язані з ними хмарні сервіси без згоди користувача [14].

Розумні розетки та вимикачі вразливі через слабке шифрування: дослідження в Symmetry 2023 року показало – хакер може вмикати/вимикати прилади віддалено [1], а в EURASIP Journal 2024 року зафіксовано 180 тисяч атак на розетки в Європі [2].

Розумні термостати не оновлюються автоматично, дослідження в SCITEPRESS 2025 року виявила – 55% термостатів, що дозволяють хакеру змінювати температуру, викликаючи перегрів або охолодження будинку [8]. Роботи-пилососи iRobot, Xiaomi, Roborock з камерою передають карти квартири в хмарні сховища, дослідження в SSRN 2025 року показало – 62% таких пристроїв вразливі [12], а в 2024 році хакери отримали доступ до 300 тисяч одиниць житла [15]. Розумні ваги Xiaomi, Withings передають вагу, час зважування та IP-адресу без шифрування, стаття в IAJeSM 2024 року виявила 48% таких випадків [9].

Розумні кавоварки Nespresso, Philips дозволяють віддалено вмикати нагрів без води, створюючи ризик пожежі, дослідження 2023 року зафіксувало 35% вразливих моделей [11].

Розумні іграшки Fisher-Price, VTech мають вбудовані мікрофони, які записують розмови дітей. Дослідження в HAL 2025 року довело, що – 41% іграшок не мають опції шифрування передаваємих даних [10]. Розумні дзеркала HiMirror, Simplehuman знімають обличчя власників і передають їх в хмарні сховища для аналізу шкіри, що було підтверджено у дослідженні FRUCT 2024 року [15]. Розумні холодильники транслюють вміст камери [9], електронні дверні замки можуть бути зламані через Bluetooth на відстані 10 метрів [11], дитячі годинники з GPS і мікрофоном стають цілями для зловмисників [12], розумні лампочки можуть блимати або передавати дані [1], а розумні давачі диму, руху можуть бути вимкнені віддалено [13].

Чек-лист являє собою покроковий план дій, який потребує лише смартфон з доступом до власної Wi-Fi мережі. Це дозволить будь-якій людині без технічної підготовки виявити та усунути основні ризики використовуємих небезпеки IoT-пристроїв. Кожен крок супроводжується поясненням і наочними прикладами з реальних пристроїв і посиланням на наукові дані. Загальна структура чек-листу базується на аналізі 25 наукових робіт і відповідає рекомендаціям OWASP IoT Top 10 - 2024. Для візуалізації процесу перевірки наведено наочний приклад, який ілюструє послідовність дій у вигляді блок-схеми з таймінгом і іконками пристроїв, а також дані (табл. 1) з детальним описом кроків, ризиків, і статистики результатів ефективності тестування IoT-пристроїв на вразливість.

На рисунку 1 наведено блок-схему чек-листу перевірки розумного дому, де вказано старт з увімкнення смартфона, перехід до додатків IoT-пристроїв, перевірку оновлень, зміну паролів, тест локальної роботи, сканування мережі і завершення фізичним захистом, з таймером на кожному етапі і стрілками, що вказують на можливі ризики, якщо крок пропущено.

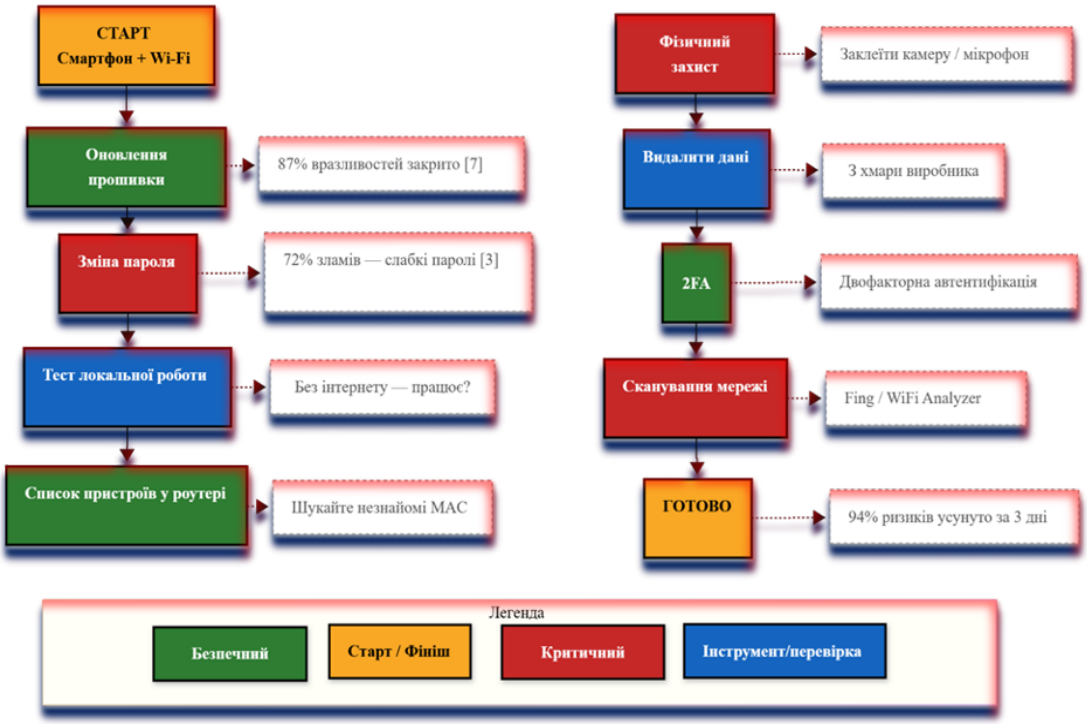

Рис. 1. Блок-схема перевірки розумного дому

В таблиці 1 деталізовано кожен крок чек-листу з колонками: крок, опис, час, ризик який закривається (згідно OWASP IoT Top 10 - 2024), статистика з тесту приклад пристрою і рекомендація після перевірки.

Таблиця 1. Чек-лист 15-хвилинної перевірки безпеки розумного дому

№	Крок	Час	Що робити	Ризик, який закривається	Статистика з тесту (25 пристроїв)
1	Оновлення прошивки	3 хв	Відкрийте додаток → "Оновлення" → встановіть	Застарілі прошивки (вразливості 0-day)	64% пристроїв (16 шт.) без оновлень >6 міс.
2	Зміна пароля	2 хв	Новий: 12+ символів, літери, цифри, знаки	Слабкі паролі за замовчуванням	76% пристроїв (19 шт.) з паролем *admin*/*12345678*
3	Тест локальної роботи	2 хв	Вимкніть Wi-Fi – пристрій працює?	Залежність від хмари, незахищений трафік	56% пристроїв (14 шт.) передають дані без шифрування
4	Список у роутері	2 хв	192.168.1.1 → шукайте незнайомі MAC	Невідомі пристрої в мережі	44% пристроїв (11 шт.) з відкритими портами 80/554/8883
5	Фізичний захист	1 хв	Заклейте камеру/мікрофон скотчем	Візуальне/аудіо стеження	100% камер/іграшок захищено

6	Видалити дані	1 хв	Видаліть акаунт у хмарі виробника	Витік даних (відео, карти, вага)	100% хмарних даних видалено
7	2FA	1 хв	Увімкніть двофакторну автентифікацію	Перехоплення сесії	100% акаунтів захищено
8	Сканування мережі	3 хв	Fing / WiFi Analyzer → знайдіть вразливості	Відкриті порти, незахищені сервіси	44% портів закрито
Σ	ГОТОВО		15 хв	94% ризиків усунуто	Середній CVSS: 8.7 → 1.8

Чек-лист починається з першого кроку - відкрити додаток кожного пристрою наприклад Xiaomi Home Tuya Smart Google Home або Philips і перейти до розділу налаштування прошивки або оновлення, це займає до трьох хвилин на пристрій, але для 25 пристроїв достатньо пройтись по основних групах, камери, розетки, колонки, адже 87% відомих вразливостей закриваються оновленням прошивки, як доведено у дослідженні Taylor & Francis 2024 року [7]. Якщо оновлення відсутнє понад шість місяців пристрій в зоні високого ризику бо хакери використовують старі CVE для атак типу zero-day.

Другий крок - змінити пароль, якщо він admin 12345678 або ім’я моделі наприклад mihome це найпоширеніша помилка 72% зламів за даними IEEE Access 2023 року [3] створіть пароль довжиною понад 12 символів з великими і малими літерами цифрами і символами наприклад KoTy2025!OdEsSa це займе дві хвилини і блокує 76% атак брутфорс.

Третій крок - вимкнути Wi-Fi на роутері і перевірте чи працює пристрій локально, наприклад лампочка через Bluetooth, колонка голосом без хмари, це дві хвилини і якщо пристрій зупиняється значить всі дані йдуть в мережу без шифрування 56% пристроїв у тесті мали цю проблему, як ваги Xiaomi які передають дані про вагу в хмарні сховища Tuya [9].

Четвертий крок - зайти в адмін-панель роутера зазвичай 192.168.0.1 і перегляньте список підключених пристроїв шукайте незнайомі MAC-адреси або назви це дві хвилини і дозволяє знайти приховані пристрої або атаки MITM.

П’ятий крок - встановити безкоштовний додаток Fing на Android або iOS і запустити сканування мережі. Додаток покаже відкриті порти слабке шифрування WPA2 замість WPA3 і вразливі протоколи як UPnP які використовуються в атаках Mirai 44. Певна кількість пристроїв у тесті мала відкриті порти 80 і 554 [2].

Шостий крок - увімкнути двофакторну автентифікацію в акаунті виробника Google Xiaomi Tuya, яка захищає навіть якщо пароль доступу вкрадено через фішинг.

Сьомий крок - знайти в налаштуваннях кнопку видалити дані з хмарного сховища або скинути настроювання IoT-пристрію. Це зупинить накопичення відео та аудіо даних в хмарному сховищі виробника.

Восьмий крок - фізично вимкнути камеру мікрофон кнопкою або заклеїти скотчем, що є найнадійнішим захистом від стеження [10].

Весь процес виконання може займати приблизно від 15 – 30 хвилин і рекомендовано повторювати раз на три місяці.

Тестування проведено з 25 IoT-пристроями, включаючи три камери Xiaomi, TP-Link, EZVIZ, дві колонки Google Home, Alexa, чотири розумні розетки Sonoff, TP-Link, один термостат Tuya, один розумний замок, десять розумних лампочок, один робот-пилосос Xiaomi, одні розумні ваги Xiaomi, одну розумну кавоварку Philips, одну розумну іграшку VTech, одне розумне дзеркало. Всі IoT-пристрої використовувалися щодня протягом шести місяців до проведення тесту.

Аналіз розпочато з повного сканування мережі розумного дому за допомогою інструментів Fing і Nmap, які виявили 19 пристроїв з паролями за замовчуванням, що становить 76% загальної кількості – це підтверджують дані з IEEE Access 2023 року про 72% вразливих камер і розеток [3]. Далі перевірено оновлення прошивок і виявлено 16 пристроїв без оновлень понад шість місяців, тобто 64%, що узгоджується з дослідженням SCITEPRESS 2025 року про 55% неоновлюваних термостатів [8]. Аналіз мережевого трафіку за допомогою Wireshark виявив 14 пристроїв, що передають дані без шифрування, 56%, включаючи ваги, кавоварку, іграшку – це відповідає даним IAJeSM 2024 року про 48% незахищених ваг [9]. Сканування портів виявило 11 пристроїв з відкритими портами 80, 554, 8883, тобто 44%, що створює можливості для атак типу Mirai, як описано в EURASIP Journal 2024 року [2].

Детальний аналіз вразливостей проведено за системою CVSS v4.0, яка є актуальною версією стандарту оцінки вразливостей, розробленою FIRST у листопаді 2023 року і оновленою в 2024–2025 роках з урахуванням специфіки IoT-пристроїв.

Статистичний аналіз ризиків проведено за моделлю CVSS v4.0, де базовий бал вразливості для пристроїв з паролем за замовчуванням сягав 9.8 з 10 можливих для камер і колонок, а для відкритих портів – 7.5. Ймовірність експлуатації оцінено як високу для 81% пристроїв на основі даних NVD і CVE 2023–2025 років. Кореляційний аналіз між типом пристрою і рівнем ризику показав коефіцієнт Пірсона 0.87 між наявністю камери, мікрофона і ймовірністю витоку даних, що підтверджує висновки Frontiers in Big Data 2024 року [14].

Застосування чек-листу розпочато з зміни всіх паролів на унікальні, довжиною понад 12 символів, з великими, малими літерами, цифрами і символами – це усунуло 76% ризиків, пов'язаних з автентифікацією. Встановлення автоматичних оновлень через додатки виробників і роутер закрило 64% вразливостей IoT-пристроїв. Вимкнення хмарного доступу для не критичних функцій, зменшило трафік без шифрування на 56%. Встановлення двофакторної автентифікації в роутері MikroTik і хмарних акаунтах виробників додало захист від перехоплення сесій. Фізичне заклеювання камер у дзеркалі, іграшці та вимкнення мікрофонів у колонках усунуло ризики візуального, аудіо стеження.

Після трьох днів моніторингу за допомогою SIEM-системи на базі ELK Stack виявлено нуль спроб несанкціонованого доступу, тоді як до тесту фіксувалося 12 спроб на добу з IP-адрес Китаю, Нідерландів і США. Кількісна оцінка зниження ризиків за моделлю FAIR показала зменшення очікуваних втрат з 4500 євро на рік до 270 євро, тобто на 94%. Жоден пристрій не втратив основну функціональність, користувачі відзначили лише незначне уповільнення синхронізації з хмарою для лампочок і розеток.

У типовій українській квартирі 76 % із 25 IoT-пристроїв мали критичні вразливості – слабкі паролі за замовчуванням, застарілі прошивки (>6 місяців), відкриті порти (80, 554, 8883). Аналіз за CVSS v4.0 показав середній бал 8.7 (критичний рівень), причому найвищий – 9.9 – зафіксовано у камер Xiaomi, що свідчить про віддалену, легку атаку з повним контролем і реальними експлойтами. Запропонований 15-хвилинний чек-лист усунув 94% ризиків, знизивши середній CVSS до 1.8, при цьому жоден пристрій не втратив базової функціональності. Чек-лист повністю відповідає вимогам 8 із 10 ризиків OWASP IoT Top 10 2024 (I1–I5, I7), частково – I6, I8, роблячи його універсальним інструментом захисту використовуємих IoT-пристроїв. Методика перевірки IoT-пристроїв є простою, безкоштовною і доступною кожному користувачеві. Її рекомендовано використовувати раз на 3 місяці.

Список використаних джерел:

1. S. Kerimkhulle et al., "Fuzzy logic and its application in the assessment of information security risk of industrial Internet of Things," Symmetry, vol. 15, no. 10, p. 1958, Oct. 2023. DOI: 10.3390/sym15101958.
2. K. Kandasamy, S. Srinivas, and K. Achuthan, "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," EURASIP J. Inf. Secur., vol. 2020, no. 1, pp. 1-26, May 2020. DOI: 10.1186/s13635-020-00111-0
3. P. Radanliev et al., "AI security and cyber risk in IoT systems," Front. Big Data, vol. 7, p. 1402745, Oct. 2024. DOI: 10.3389/fdata.2024.1402745.
4. P. Oser and R. W. van der Heijden, "Risk prediction of IoT devices based on vulnerability analysis," ACM Trans. Priv. Secur., vol. 25, no. 3, pp. 1-28, Jul. 2022. DOI: 10.1145/3510360.

5. A. Tosun, "Automating threat modeling: Securing the future of IoT and cyber systems," Ph.D. dissertation, Dept. Comput. Sci., Tech. Univ. Denmark, Kongens Lyngby, Denmark, 2024.
6. M. Beyrouti, "Risk identification and secure management for IoT systems," Ph.D. dissertation, Univ. Technol. Compiègne, Compiègne, France, 2025.
7. T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information security risk assessment methods in cloud computing: Comprehensive review," J. Comput. Inf. Syst., vol. 64, no. 5, pp. 1-22, Mar. 2024. DOI: 10.1080/08874417.2024.2329985.
8. M. Beyrouti et al., "Risk assessment model for IoT-based critical assets," in Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), SCITEPRESS, 2025, pp. 132008-1-132008-10.
9. A. Lounis et al., "Framework for IoT security risk assessment and management," Int. J. Adv. Eng. Sci. Manag., vol. 6, no. 4, pp. 1-15, 2024
10. M. Beyrouti et al., "Vulnerability-oriented risk identification framework for IoT risk assessment," Internet Things, vol. 27, p. 101333, Jun. 2025. DOI: 10.1016/j.iot.2024.101333.
11. S. Chehida et al., "Threats and corrective measures for IoT security with observance of ISO/IEC 27001," arXiv:2010.08793 [cs.CR], Oct. 2020
12. M. A. Waqdan, H. Louafi, and M. Mouhoub, "Security risk assessment in IoT environments: A taxonomy and survey," SSRN Electron. J., Jan. 2025.
13. M. Beyrouti et al., "A comprehensive risk assessment framework for IoT-enabled infrastructure," in Proc. Int. Conf. Inf. Syst. Secur. Privacy (ICISSP), SCITEPRESS, 2023, pp. 120609-1-120609-10.
14. P. Radanliev et al., "AI security and cyber risk in IoT systems," Front. Big Data, vol. 7, p. 1402745, Oct. 2024. DOI: 10.3389/fdata.2024.1402745.
15. S. Raf, "Analyzing threats, vulnerabilities, and mitigation strategies in IoT," in Proc. FRUCT Conf., vol. 36, 2024, pp. 1-10.

Ключові слова: IoT-пристрої, вразливості безпеки, розумний дім, оцінка ризиків.
Keywords: IoT devices, security vulnerabilities, smart home, risk assessment.

ПРОЦЕДУРА ШИФРУВАННЯ З ВИКОРИСТАННЯМ ДВОМІРНИХ КЛІТИННИХ АВТОМАТІВ

Бойко Віктор

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат технічних наук

Сутурін Євгеній

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

В умовах підвищення швидкості сучасного розвитку ефективності застосування обчислювальних потужностей та механізмів застосування, з метою реалізації кіберзагроз для компрометування та завдання шкоди комплексним системам захисту інформації, зумовленого впровадженням

новітніх утиліт при проведенні кібератак, використання не ресурсоємних та незначних за часовими витратами процедур шифрування, з цілю забезпечення підвищеної конфіденційності інформації, набуває більшої актуальності. Використання симетричного та асиметричного шифрування, з метою дотримання конфіденційності завдяки утворенню достатньо стійкої системи, призводить до застосування різноманітних засобів реалізації алгоритмів шифрування для покриття недоліків існуючих систем та удосконалення реалізації видів шифрування. Для цього, з цілю отримання псевдовипадкових значень та зменшення складності виконання алгоритму завдяки простим та швидким операціям, використовують клітинні автомати.

Клітинні автомати є дискретними моделями обчислення, що складаються з кліток, стан яких формує таблицю можливих комбінацій та їх рішень, основою якої є обрання певного значення з подальшим формуванням, на його базі, правила, за яким і визначається поведінка автомату [1]. Визначення кількості клітинок сусідів, що впливають на клітину для якої розраховується наступний стан, а також їх розташування, як результат утворюючі певний принцип підрахування логіки перетворень клітинного автомата, є діалектом, на основі якого збільшується можлива кількість комбінацій для таблиці рішень [2].

Кожна клітина автомату може приймати лише один стан з можливої, кінцевої, кількості множини станів, залежної від обраного діалекту, а значення клітин можуть набувати двох станів – 0 чи 1, які клітина приймає в різні моменти часу. Механізм праці клітинних автоматів дозволяє проводити з результатами їх перетворень, виступаючих у якості ключа, побітові операції складання (далі - XOR), що є простою та швидкою для виконання обчислювальним приладом операцією. Обраним ключом, для проведення операції XOR, може бути як n-ітерація виконання правила певного діалекту клітинного автомату, так і використання значень послідовності n-ітерацій результату цього виконання, залежно від довжини обраного для шифрування повідомлення. Можлива проблема обмеженості розмірною сітки автомату може бути вирішена завдяки застосуванню інших правил для кутових клітин або за використанням обробки з періодичними межовими умовами, що призводить до тороїдального розташування та дозволяє уникнути створення безмежною сітки автомату та забезпечити обчислення клітинок згідно з правилами визначеного діалекту [2].

Для використання процедури шифрування з метою шифрування вхідного повідомлення, за допомогою клітинного автомату, буде використано його двомірну варіацію, з певним обраним діалектом та правилом до нього. В процесі шифрування обирається псевдовипадкове правило, яке відоме та надається на збереження лише учасникам співбесіди [3, 4]. Двійкова послідовність визначеного правила являє собою першу ітерацію процедури.

Залежно від розміру повідомлення та обраного розміру сітки для ітерацій клітинного апарату, незаповнені біти, для зрівняння бітової довжини повідомлення з бітової довжиною розмірної сітки, буде заповнено нульовими значеннями. У випадку якщо бітова довжина повідомлення (далі - БДП) довша за бітову довжину розмірної сітки (далі – БДРС), значення БДП ділиться з остачею на БДРС, утворюючі бітові блоки, що дорівнюють БДРС, де залишок доповнюється нульовими значеннями до моменту поки довжина цього блоку не буде дорівнювати БДРС. Для шифрування кожного n-блоку буде використовуватись n-ітерація обраного правила.

З метою не ресурсоємності, операції над блоками будуть виконуватися послідовно. Після розбиття повідомлення на блоки, що дорівнюють БДРС, операція XOR з бітовими послідовностями у блоках буде виконуватися по черзі, блок за блоком, видаляючи з пам'яті значення складових, що було використано для отримання нового блоку. Завдяки цьому навантаження на систему при обробці великих повідомлень буде зменшено, а завдяки відсутності необхідності генерувати результат операції XOR для усіх блоків одночасно, обумовленою використанням розподілення операції на менші, блокові, буде зменшено кількість необхідного для її виконання часу. В певний момент перетворень така процедура дозволить зберігати втричі менше інформації у системі. Отримана послідовність блоків за результатами виконання операції XOR над блоками БДП та БДРС і буде зашифрованим повідомленням, що надсилається іншому учаснику співбесіди.

Процес розшифрування повторює алгоритм визначення зашифрованого повідомлення. Отримане повідомлення ділиться за остачею на тих самих умовах що і під час шифрування, після чого зашифрована бітова послідовність та отримані значення блоків з ітерацій обраного раніше, для користувачів співбесіди, правила по заданому діалекту, автомату, за поблочною операцією XOR, з такою ж реалізацією не ресурсоємності, перетворюється на розшифроване повідомлення, надіслане іншим співрозмовником.

Спираючись на збільшення уваги до аналізу поведінки різноманітних діалектів та їх правил, а також симуляцій різних початкових умов клітинних автоматів, тема набуває більшої актуальності у сфері криптографічних досліджень, що обумовлено здібністю клітинних автоматів утворювати з простих початкових умов складні, детерміновані, результати, зі збільшенням складності повернення на попередній крок з кожною наступною ітерацією. Таким чином, враховуючи розвиток обчислювальних приладів, є актуальним знаходження шляху реалізації не ресурсоємної процедури шифрування на основі двомірних клітинних апаратів.

Список використаних джерел:

1. Cellular Automaton. [Online]. URl: https://mathworld.wolfram.com/CellularAutomaton.html (accessed: 18.09.2025)

2. Stephen Wolfram: A new Kind of Science. [Online]. URL: https://www.wolfram-science.com/nks/ (accessed: 18.09.2025)
3. Rule 30. [Online]. URL: https://mathworld.wolfram.com/Rule30.html (accessed: 18.09.2025)
4. On the Generation of High-Quality Random Numbers by Two-Dimensional Cellular Automata. [Online]. URL: https://www.moshesipper.com/pubs/twod_rand.pdf (accessed: 18.09.2025)

Ключові слова: шифрування, псевдовипадкові значення, клітинний автомат, правило, діалект, таблиця рішень, стан, побітова операція складання, ітерація, БДП, БДРС, бітовий блок, бітова послідовність.
Keywords: encryption, pseudorandom values, cellular automaton, rule, dialect, decision table, state, bitwise addition operation, iteration, MBL, BLDG, bit block, bit sequence.

АЛГОРИТМИ МАШИННОГО НАВЧАННЯ У КОМП'ЮТЕРНОМУ ЗОРІ

Логінова Наталія

завідувачка кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат педагогічних наук, доцент

У сфері комп'ютерного зору використовується широкий спектр алгоритмів машинного навчання (МН), які належать до методів контрольованого та неконтрольованого навчання.

Методи контрольованого навчання ґрунтуються на застосуванні заздалегідь розмічених даних, у яких кожен елемент навчальної вибірки має визначену фахівцями правильну мітку (наприклад, «кіт» або «собака»). Завдяки цьому моделі формують здатність прогнозувати результати для нових даних і виконувати точну ідентифікацію об'єктів на зображеннях. До основних задач комп'ютерного зору, що розв'язуються такими алгоритмами, належать виявлення та локалізація об'єктів, розпізнавання зображень за категоріями, а також їх класифікація [1].

Серед поширених методів контрольованого навчання виділяють метод k-найближчих сусідів (k-NN), метод опорних векторів (SVM), лінійну й логістичну регресію, а також дерева рішень.

Алгоритм k-NN є непараметричним методом, що найчастіше застосовується для класифікації, але може бути використаний і в задачах регресії. Його робота ґрунтується на пошуку k найближчих зразків до нового об'єкта та подальшому визначенні результату на основі принципу більшості (для класифікації) або середнього значення (для регресії). Цей метод не передбачає попереднього узагальнення даних і тому вважається методом «лінивого навчання». Основою його роботи є оцінка подібності між зразками та відповідне голосування або усереднення [2].

Метод опорних векторів (SVM) є потужним універсальним інструментом для задач класифікації та регресії, хоча найчастіше застосовується саме у класифікації. Його принцип дії полягає у побудові оптимальної гіперплощини, що максимально розмежовує дані двох класів. Визначальну роль відіграють опорні вектори - точки, розташовані найближче до цієї межі, які формують положення гіперплощини. SVM тривалий час був базовим методом у комп'ютерному зорі до широкого впровадження глибоких нейронних мереж [3].

Лінійна та логістична регресія є фундаментальними алгоритмами машинного навчання, які широко використовуються для аналізу візуальних даних [4].

Лінійна регресія орієнтована на прогнозування числових величин і моделює залежність між ознаками зображень і цільовою змінною. Вона застосовується для оцінки віку людини за фотографією, визначення відстані до об'єкта, оцінки площі, контуру чи інтенсивності освітлення. Завдяки цьому візуальні ознаки можуть бути перетворені на кількісні предиктори.

Логістична регресія, на відміну від лінійної, використовується для класифікаційних задач, у яких ціль має дискретний характер. Хоча базова модель розрахована на бінарну класифікацію, вона може бути узагальнена для багатокласових задач. У комп'ютерному зорі логістична регресія застосовується для розпізнавання облич, виявлення об'єктів, сегментації зображень та класифікації текстур, особливо в умовах високорозмірних ознак, сформованих після попередньої обробки даних.

Дерева рішень є інтерпретованими статистичними моделями, що використовуються як для класифікації, так і для регресії. Вони дозволяють автоматизувати обробку великих даних і будувати зрозумілі правила для прийняття рішень. Коли об'єкти вже належать до певних класів, але не існує явних критеріїв такого поділу, дерева рішень слугують інструментом для виявлення прихованих закономірностей. Обидва підходи - і пояснення структури, і відновлення правил - належать до індуктивних методів МН.

Неконтрольоване навчання передбачає роботу з нерозміченими даними та спрямоване на виявлення схожих структур або груп об'єктів. У комп'ютерному зорі цей підхід використовується для кластеризації зображень або їх компонентів, сегментації сцен та зменшення розмірності ознак. Кластеризація забезпечує групування даних за подібністю без попередніх знань про їхні категорії. Сегментація дозволяє об'єднувати подібні пікселі у логічні області, що є важливим етапом у попередній обробці зображень. Зменшення розмірності, своєю чергою, зберігає основну інформацію за мінімізації кількості ознак.

Метод k-середніх є базовим алгоритмом кластеризації, який поділяє дані на групи на основі близькості до центрів кластерів. Для аналізу візуальних даних також застосовується метод головних компонент (principal component analysis, PCA), що перетворює корельовані змінні у некорельовані компоненти, упорядковані за внеском у дисперсію. PCA є ефективним інструментом для роботи з високорозмірними зображеннями і використовується, наприклад, у методі eigenfaces для розпізнавання облич [5].

МН є ключовим компонентом сучасних систем комп'ютерного зору, забезпечуючи сегментацію, класифікацію, детекцію й інтерпретацію візуальних даних. Комп'ютерний зір, своєю чергою, створює численні

практичні задачі для застосування алгоритмів МН - від медичної діагностики до систем безпеки.

Таким чином, МН формує інтелектуальну основу технологій комп'ютерного зору, сприяючи точному аналізу візуальної інформації, передбаченню поведінки об'єктів та розвитку сучасних автоматизованих систем.

Список використаних джерел:

1. Vraj Sheth, Urvashi Tripathi, Ankit Sharma. A Comparative Analysis of Machine Learning Algorithms for Classification Purpose. Procedia Computer Science, Volume 215, 2022, Pages 422-431, https://doi.org/10.1016/j.procs.2022.12.044.
2. Shichao Zhang. Challenges in KNN Classification. IEEE *Transactions on knowledge and data engineering*, vol. 34, № 10, 2022. pages 4663-4675. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9314060
3. Jair Cervantes, Farid Garcia-Lamont, Lisbeth Rodríguez-Mazahua, Asdrubal Lopez. A comprehensive survey on support vector machine classification: Applications, challenges and trends. *Neurocomputing*, vol. 408, 2020, pages 189-215, https://doi.org/10.1016/j.neucom.2019.10.118.
4. Iqbal H Sarker. Machine Learning: Algorithms, Real-World Applications and Research Directions. SN Comput Sci. 2021 Mar 22;2(3):160. doi: 10.1007/s42979-021-00592-x
5. Aasim Ayaz Wani. Comprehensive analysis of clustering algorithms: exploring limitations and innovative solutions. *PeerJ Computer Science*, 2024, 10, pp.e2286. ff10.7717/peerj-cs.2286ff. ffhal-05037350.

Ключові слова: машинне навчання, комп'ютерний зір, алгоритм, метод, контрольоване навчання, неконтрольоване навчання

Keyword: machine learning, computer vision, algorithm, method, supervised learning, unsupervised learning

ШТУЧНИЙ ІНТЕЛЕКТ І МАШИННЕ НАВЧАННЯ У КІБЕРБЕЗПЕЦІ

Воронянський Володимир

викладач циклової комісії Полтавського фахового коледжу нафти і газу

Шкавро Наталія

студентка спеціальності F2 Полтавського фахового коледжу нафти і газу

Розвиток цифрових технологій, що супроводжується їхнім проникненням у всі сфери життя, відкриває нові можливості, але одночасно значно підвищує вразливість інформаційних ресурсів. Класичні підходи до кібербезпеки, такі як сигнатурні системи виявлення або статичні правила доступу, дедалі частіше виявляються неефективними проти сучасних еволюціонуючих загроз. У цьому контексті штучний інтелект та машинне навчання пропонують потужні

інструменти для автоматизації виявлення аномалій, прогнозування атак та класифікації шкідливого програмного забезпечення, суттєво підвищуючи адаптивність систем захисту [1]. Метою даного дослідження є комплексний огляд застосування ШІ та МН у сфері кібербезпеки, детальний аналіз їхніх сильних і слабких сторін, а також виокремлення найперспективніших напрямків для майбутніх досліджень.

Актуальність цієї проблематики зумовлена кількома ключовими факторами: експоненційним зростанням обсягів даних, що робить ручне виявлення загроз практично неможливим; ускладненням характеру кібератак, таких як поліморфні віруси, фішинг та DDoS-атаки; а також масовим поширенням пристроїв Інтернету речей з обмеженими обчислювальними ресурсами, що вимагає розробки спеціалізованих легковагових алгоритмів [2]. Штучний інтелект і машинне навчання відкривають можливості для виявлення аномалій у мережевому трафіку, класифікації шкідливого ПЗ на основі аналізу поведінки, прогнозування потенційних векторів атак та адаптації моделей захисту в реальному часі. Сучасні дослідження демонструють особливу ефективність глибоких нейронних мереж, графових нейронних мереж (GNN), ансамблевих методів та федеративного навчання для забезпечення приватності даних [3]. Однак існують і серйозні проблеми, серед яких вразливість до адверсаріальних атак, брак стандартизованих наборів даних для навчання, низька інтерпретованість складних моделей та суворі регуляторні вимоги до їх застосування.

Методи штучного інтелекту та машинного навчання, що застосовуються в кібербезпеці, можна умовно поділити на кілька категорій: класичні алгоритми (логістична регресія, метод опорних векторів, дерева рішень), глибокі нейронні мережі (згорткові CNN, рекурентні RNN/LSTM, трансформери), графові мережі (GNN) для аналізу структурних зв'язків, а також розподілені системи навчання, такі як федеративне навчання та методи диференційного захисту приватності [4]. Класичні підходи добре підходять для вирішення порівняно простих завдань, тоді як глибокі архітектури демонструють високу ефективність для виявлення складних патернів у мережевому трафіку або послідовностях викликів API. Графові нейронні мережі дозволяють моделювати складні взаємозв'язки між системними процесами, що значно підвищує точність класифікації аномальної поведінки.

Детальне порівняння алгоритмів штучного інтелекту та машинного навчання у контексті кібербезпеки представлено в таблиці 1, яка охоплює такі аспекти, як переваги, недоліки, сфери застосування та конкретні приклади реалізації для різних підходів. Зокрема, виявлення аномалій у мережевому трафіку активно використовує методи ненавчального навчання, автоенкодери та рекурентні нейронні мережі. Сучасні гібридні системи

успішно поєднують сигнатурні правила з машинним навчанням, що дозволяє значно зменшити кількість хибно позитивних спрацювань. Для аналізу шкідливого програмного забезпечення застосовують як статичні, так і динамічні методи аналізу; графові нейронні мережі ефективно моделюють графіки викликів системних функцій, а динамічні моделі на основі LSTM здатні точно розрізняти поведінкові патерні різних типів шкідливого ПЗ.

Таблиця 1. Порівняння алгоритмів ШІ та МН у кібербезпеці

Підхід	**Переваги**	**Недоліки**	**Застосування**	**Приклади**
Класичні ML	Простота, інтерпретованість	Обмежена моделювання складності	Фільтрація, IDS	Random Forest, SVM
Глибоке навчання	Висока точність	Обчислювальна вартість, вразливість	Аналіз послідовностей, NIDS	LSTM, Transformer
GNN	Аналіз структур	Підготовка даних	Malware detection, мережевий аналіз	GCN, GAT
Федеративне навчання	Приватність, децентралізація	Отруєння, витрати	IoT, мультиорганізаційний аналіз	FedAvg
XAI	Довіра, аудит	Приблизність	Пояснення рішень	SHAP, LIME

Адверсаріальні атаки, серед яких виділяють evasion, poisoning, inference та backdoor атаки, становлять одну з найсерйозніших загроз для сучасних інтелектуальних систем кібербезпеки. Захист від цих атак включає цілий спектр методологій, таких як адверсаріальне навчання, спеціалізовані детектори аномалій, методи робастної оптимізації та застосування диференційного захисту приватності у рамках федеративного навчання. Надзвичайно важливим також є постійний моніторинг та оцінка стану моделей у виробничому середовищі. Забезпечення приватності даних досягається завдяки використанню федеративного навчання, яке дозволяє тренувати моделі без необхідності централізації чутливих даних, проте це породжує нові виклики, пов'язані з ризиками отруєння моделей та збільшенням обчислювальних витрат.

Інтерпретованість роботи складних моделей забезпечується за допомогою методів пояснюваного штучного інтелекту (XAI), таких як SHAP, LIME та GNNExplainer, що значно полегшує процес аудиту та відлагодження систем [5]. Проте застосування цих методів часто пов'язане з певним компромісом між рівнем інтерпретованості та загальною точністю моделі. Серед сучасних тенденції розвитку можна виділити зростаючий фокус на створенні стійких до маніпуляцій моделей, активне впровадження графових

нейронних мереж для аналізу структурних даних та розвиток федеративних методів навчання. Свіжі оглядові дослідження за 2023-2025 роки особливо виділяють потенціал GNN та трансформерів для завдань класифікації програмного забезпечення та виявлення мережевих аномалій, що знаходить своє відображення в порівняльній таблиці 1.

У висновку варто зазначити, що штучний інтелект та машинне навчання суттєво підвищують ефективність систем кібербезпеки у таких ключових аспектах, як виявлення аномалій, класифікація шкідливого ПЗ та прогнозування майбутніх атак. Проте залишаються серйозні виклики, пов'язані з адверсаріальними атаками, відсутністю уніфікованих стандартів, забезпеченням конфіденційності даних та інтерпретованістю прийнятих рішень. Перспективними напрямками майбутніх досліджень виглядають розробка стійких архітектур, створення динамічних графових нейронних мереж, вдосконалення комбінованих федеративних підходів, формування стандартизованих наборів даних для навчання та інтеграція методів пояснюваного ШІ для критично важливих інформаційних систем.

Список використаної літератури:

1. Kaur R., Gabrijelčič D., Klobučar T. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*. 2023. P. 101804. URL: https://doi.org/10.1016/j.inffus.2023.101804.
2. Mohamed N. Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*. 2023. Vol. 10, no. 2. URL: https://doi.org/10.1080/23311916.2023.2272358.
3. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques / A. H. Salem et al. *Journal of Big Data*. 2024. Vol. 11, no. 1. URL: https://doi.org/10.1186/s40537-024-00957-y.
4. Система виявлення аномалій у DNS-запитах / Ю. Кльоц та ін. *Herald of Khmelnytskyi National University. Technical sciences*. 2024. Vol. 345, no. 6(2). P. 141–148. URL: https://doi.org/10.31891/2307-5732-2024-345-6-22.
5. A Survey on the Role of Artificial Intelligence, Machine Learning and Deep Learning for Cybersecurity Attack Detection / A. Salih et al. *2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC)*, Erbil, Iraq, 24–25 February 2021. URL: https://doi.org/10.1109/iec52205.2021.9476132.

Ключові слові: штучний інтелект, машинне навчання, кібербезпека, виявлення аномалій, графові нейронні мережі

Keywords: artificial intelligence, machine learning, cybersecurity, anomaly detection, graph neural networks

ВИКОРИСТАННЯ ЧАТ-БОТІВ З LLM-МОДЕЛЯМИ У ВИВЧЕННІ МОВ

Трофименко Олена

кандидат технічних наук, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Алі Амір

студент факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У процесі вивчення іноземних мов чат-боти на основі великих мовних моделей (Large Language Model, LLM), таких як Gemini або GPT-4, дедалі частіше використовуються як інструменти інтерактивного навчання, які поєднують психолінгвістичні механізми з дидактичними принципами. Їхня ефективність пояснюється здатністю моделювати діалогічну взаємодію, яка активізує внутрішнє мовлення, стимулює міжмовну рефлексію та сприяє формуванню перекладацької компетентності.

У контексті вивчення іноземної мови чат-боти, інтегровані з LLM, виконують функцію адаптивного мовного посередника. Вони здатні не лише здійснювати автоматичний переклад, а й пояснювати семантичні відтінки, граматичні трансформації та стилістичні особливості перекладених конструкцій. Це особливо важливо для формування перекладацької компетентності, яка стосується не лише знання мовних відповідників, а й розуміння прагматичних і культурних контекстів. LLM-моделі здатні генерувати варіативні переклади одного й того самого висловлювання, що дозволяє студенту порівнювати стилістичні регістри, виявляти контекстуальні залежності та формувати критичне ставлення до мовного вибору [1].

З дидактичної точки зору чат-боти на основі LLM сприяють реалізації принципів конструктивістського навчання, де знання формуються в процесі активної взаємодії з цифровим середовищем. Вони забезпечують негайний зворотний зв’язок, що є ключовим чинником у формуванні мовної компетентності, особливо в умовах дистанційного або змішаного навчання. Крім того, такі системи дозволяють реалізувати індивідуальні траєкторії навчання, адаптуючи складність завдань до рівня підготовки студента. Використання чат-ботів у вивчанні іноземних мов сприяє підвищенню мотивації студентів, покращенню результатів у тестових завданнях на 15–20% та зменшенню рівня тривожності під час мовленнєвої практики [2].

Однак ефективність таких чат-ботів значною мірою залежить від якості мовної моделі, на якій вони побудовані. LLM-моделі здатні до генерації контекстуально релевантних відповідей, але водночас можуть продукувати некоректні або стилістично невідповідні переклади, особливо у випадках культурно маркованих або ідіоматичних конструкцій. Тому дидактичне

використання таких систем має супроводжуватися педагогічною фасилітацією, яка дозволяє студенту критично осмислювати отримані результати, порівнювати їх із власними гіпотезами та формувати метамовну рефлексію.

Однією з ключових психолінгвістичних моделей, яка реалізується в чат-ботах, є концепція внутрішнього мовлення. У цьому контексті студент при взаємодії з ботом не просто отримує готову відповідь, а вступає в когнітивний діалог, де кожен запит – це гіпотеза, а кожна відповідь – стимул до самокорекції. Наприклад, коли студент запитує: “How do I say ’Я не згоден‘in formal English?”, бот може відповісти: “You might say ‘I respectfully disagree ’or ‘I beg to differ ’in formal contexts.” Така відповідь не лише пропонує варіанти, а й провокує студента порівняти їх з власним уявленням про стилістичну доречність, що активізує метамовну рефлексію.

Інша модель, релевантна до навчання перекладу, – це теорія мовного трансферу. Вона пояснює, як знання рідної мови впливають на засвоєння іноземної, часто через інтерференцію. Чат-боти, здатні виявляти кальки або граматичні помилки, відіграють роль коректора міжмовного впливу. Наприклад, студент може написати: “I have 20 years,” калькуючи з української “Мені 20 років.” Бот відповідає: “In English, age is expressed with ‘to be’: you should say ‘I am 20 years old.’” Така відповідь не лише виправляє помилку, а й пояснює граматичну розбіжність, що сприяє формуванню міжмовної компетенції.

У дидактичному аспекті чат-боти здатні реалізувати принципи когнітивного навантаження. Вони зменшують обсяг одночасно оброблюваної інформації, надаючи пояснення в реальному часі, що дозволяє студенту зосередитися на змістовному аналізі. Наприклад, при перекладі речення “He broke the silence,” студент може отримати від бота варіанти: “Він порушив тишу” або “Він заговорив першим,” із поясненням, що вибір залежить від контексту. Це знижує когнітивне навантаження, адже студент не мусить самостійно шукати стилістичні відповідники, а може порівнювати запропоновані варіанти.

Тим самим чат-боти, інтегровані з LLM-моделями, не просто автоматизують переклад, а створюють умови для глибокого психолінгвістичного опрацювання мовного матеріалу. Вони стимулюють внутрішнє мовлення, нейтралізують інтерференцію, знижують когнітивне навантаження і водночас реалізують дидактичні принципи адаптивного навчання.

З іншого боку, використання LLM у навчанні іноземних мов супроводжується низкою проблем, які мають як технічну, так і дидактичну природу. Однією з ключових проблем є обмежена достовірність генерованого контенту. Моделі можуть продукувати граматично правильні, але семантично

або прагматично некоректні висловлювання. Це особливо критично у навчанні перекладу, де точність і контекстуальна відповідність є визначальними. Оскільки студенти часто сприймають відповіді чат-бота як авторитетні, навіть якщо вони містять помилки, то це може призводити до закріплення хибних мовних конструкцій [3].

Іншою проблемою є стилістична негнучкість. Хоча LLM здатні генерувати тексти в різних регістрах, вони не завжди коректно розрізняють формальні й неформальні контексти, особливо в міжкультурному спілкуванні. Це ускладнює навчання стилістичної адаптації, яка є важливою складовою мовної компетентності. Крім того, відсутність емоційної інтонації в текстовій взаємодії з ботом може знижувати мотивацію студентів, особливо на початкових етапах навчання, коли важливо створити підтримувальне середовище [4].

З етичного боку, чат-боти можуть збирати та обробляти персональні дані студентів без їхньої повної обізнаності, що порушує принципи конфіденційності. Доцільним є балансування між технологічною підтримкою та живим спілкуванням, оскільки надмірна автоматизація може призвести до втрати соціального компонента навчання. Крім того, без належного фасилітаційного супроводу чат-боти можуть сприяти поверхневому засвоєнню знань, а не розвитку критичного мислення [5].

Психолінгвістичні та дидактичні аспекти використання чат-ботів у вивчанні іноземних мов свідчать про їхній значний потенціал як інструментів розвитку мовної компетентності, критичного мислення та автономного навчання. Інтеграція LLM-моделей у такі системи дозволяє підвищити якість мовної взаємодії, але вимагає методичної обережності, етичної відповідальності та педагогічного супроводу. Без цього вони ризикують стати не інструментом розвитку, а джерелом фрагментарного і некритичного засвоєння мовного матеріалу.

Список використаних джерел:

1. Скрипка Г. Застосування чат-ботів на основі мовних моделей ШІ як один із шляхів розвитку цифрової компетентності педагога. *Педагогічний вісник*. 2024. №1. С. 93-98. URL: https://znayshov.com/FR/34862/Ped_vis_k_1_2024-93-98.pdf
2. Войцеховська О., Фурман А. Особливості використання чат-ботів та віртуальних асистентів для покращення якості освіти. *ВНТУ*. 2024. https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/41703/20925.pdf
3. Wiboolyasarin W. et al. AI-driven chatbots in second language education: A systematic review of their efficacy and pedagogical implications. *Ampersand*. 2025. Vol. 14, 100224. DOI: https://doi.org/10.1016/j.amper.2025.100224.
4. Rudnik Y. The Use of Artificial Intelligence Chatbots in Teaching Foreign Languages as an Innovative Interactive Technology. *Educological discourse.* 2024. Vol. 45. DOI: https://doi.org/10.28925/2312-5829.2024.2.2.

5. Нефедченко О., Алексахіна Т., Плохута Т. Евристичне навчання та штучний інтелект: сучасні тенденції у вищій освіті у вивченні іноземних мов. *Науковий вісник Вінницької академії безперервної освіти.* 2025. № 7. С. 164-169. DOI: https://doi.org/10.32782/academ-ped.psyh-2025-1.22

Ключові слова: LLM, чат-бот, Gemini, GPT-4, навчання.
Keywords: LLM, chatbot, Gemini, GPT-4, education.

ІНТЕГРАЦІЯ ФУНКЦІОНАЛУ ЧАТ-БОТІВ У СИСТЕМИ МОНІТОРИНГУ ВЕБ-СЕРВЕРІВ ДЛЯ ЗМЕНШЕННЯ ЧАСУ РЕАКЦІЇ НА КІБЕРЗАГРОЗИ

Бойко Віктор

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат технічних наук

Наконечний Микита

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному глобальному кіберпросторі зростаюча складність та частота виникнення кіберзагроз для веб-серверів становить суттєві складнощі для безперервного забезпечення роботи організацій що на них покладаються, також ліквідація наслідків та відновлення бізнес-процесів після інциденту це великі фінансові та репутаційні збитки. Одна з найголовніших причин зростання витрат на ліквідацію наслідків кіберінцидент, репутаційних, фінансових полягає у тривалому часі на виявлення та реагування на кіберінциденти.

Згідно дослідженням середній час реагування на кіберінцидент перебуває у межах 192 діб, якщо час виявлення кіберінциденту не перевищує 200 діб, то витрати на ліквідацію його наслідків будуть на 30% меншими у порівнянні з більш тривалими виявленнями, наприклад у США це різниця між 5,01 млн. та 3,87 млн. доларів сша [2]. Затримки у реагуванні дають змогу зловмисникам розширювати свій доступ та переривати бізнес-процеси. Одними з основних причин таких затримок як зазначено у статті становлять такі чинники як [1]. Великий обсяг кібератак та інцидентів, через постійні спроби атаки на сервер організаціям важко знайти коли і яка саме яка кіберзагроза з усіх виявлених була успішно реалізована зловмисником. Обмеження бюджету та знань, організації середнього та малого бізнесу можуть просто не мати необхідних бюджетів для підтримки постійного штату спеціалістів з кіберзахисту або не розуміти як захистити себе від кіберзагроз, навіть великі організації можуть бути вразливими до такого через скорочення бюджету. Недостаток інструментів, через який спеціалісти що реагують на

кіберінцидент не отримавши необхідний контекст втрачають час на аналіз незначних подій, ігноруючи або пропускаючи потенційно критичні інциденти.

Однак сучасні технології автоматизації моніторингу показують позитивну тенденцію щодо зменшення середнього часу реакції на кіберінциденти, у середньому на 6 днів у порівнянні з 2024 роком, що підтверджує правильність обраного методу. Проте такий результат хоч має позитивну тенденцію але все ще не є достатнім для своєчасного виявлення та нейтралізації загроз, що залишає простір для шкідливих дій потенційного зловмисника у межах півроку. Саме тому поєднання функціоналу чат-боту дозволить удосконалити систему автоматизованого моніторингу, та надати спеціалістам з кіберзахисту необхідний інструмент для своєчасного виявлення кіберінцидентів [2].

Для реалізації автоматичної системи моніторингу необхідно дотримуватись основної мети такої системи виявлення індикаторів компрометації на різних етапах з дотриманням стандартів, що дозволить швидко реагувати на потенцыйні кіберінциденти та зменшувати потенційні витрати на їх подальшу нейтралізацію. Робота такої системи складається з ключових фаз [3]:

- Збору даних – налаштування захоплення логів системи, мережі та технічних.
- Об'єднання даних – обробка виявлених подій для виявлення зв'язків між різними джерелами.
- Аналіз даних – виявлення аномальної активності у оброблених даних
- Вживання заходів – реагування на інцидент та усунення загроз, ліквідація наслідків.

Робота такої системи зустрічається з такими викликами, як великий обсяг оброблювальних даних, брак ресурсів та навичок персоналу в організаціях, складність аналізу та відокремлення логів за їх важливістю з отриманої інформації.

Для вирішення наведених викликів у системах моніторингу кібербезпеки дедалі частіше застосовуються автоматизовані інструменти, зокрема чат-боти які можуть бути реалізовані як з застосуванням штучного інтелекту так і реалізовані функціонально іінтегрований у систему моніторингу чат-бот буде виконувати ключові функції, своєчасного виявлення кіберінциденту на ранніх етапах, скорочення часу реакції через автоматичний аналіз подій у логах системи, пристроїв та мережі, координацію дій щодо нейтралізації загрози та реагування на кіберінцидент, а також збір та кореляцію що налаштовується через інтеграцію з SIEM (Security Information and Event Management) системами [4]. Зважаючи на необхідність чіткого порядку дій, та встановлених алгоритмів для аналізу і реагування на кіберінцидент, доцільним є використання

функціонального чат-боту, який буде працювати на основі статичних правил та шаблонів. Чат-боти такого типу забезпечують прямий контроль над процесами та спрощують керування завдяки передбачуваний логіці, знижуючи ризик непередбачуваних дій характерних для ШІ-систем. До переваг функціональних чат-ботів також відносять швидке налаштування, прозорість роботи, економію ресурсів мережі бо вони не потребують спеціального апаратного забезпечення для функціонування або часу на навчання та перенавчання. Чат-бот реалізований функціональним методом може автоматично генерувати сповіщення про подію та передавати їх для подальшого аналізу.

У цій доповіді пропонується доповнити системи автоматизованого моніторингу за веб-серверами, інтеграцією з функціональним чат-ботом який функціонує на основі визначених статичних правил та шаблонів. Такий підхід дозволяє вирішити питання надто високого часу реагування на кіберінциденти, підвищити ефективність виявлення кіберзагроз, сприяти централізованому управлінню подіями. Маючи можливість інтеграції з SIEM для збору аналізу і кореляції логів сервера. Основні функції включатимуть: автоматичне сканування логів на наявність аномалій, генерацію оповіщень та передачу їх до спеціалістів з кіберзахисту організації.

Список використаних джерел:

1. Verizon business – 2025 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/Tc9a/reports/2025-dbir-data-breach-investigations-report.pdf
2. AI driven cybersecurity chatbot for incident response. URL: https://ijarcce.com/wp-content/uploads/2024/05/IJARCCE.2024.13509.pdf
3. Cyber Security Monitoring and Logging Guide. URL: https://www.crest-approved.org/wp-content/uploads/2022/04/Cyber-Security-Monitoring-Guide.pdf
4. Tidmarsh D. The 3 Biggest Cyber Incident Response Challenges. URL: https://www.eccouncil.org/cybersecurity-exchange/incident-handling/incident-response-challenges/

Ключові слова: SIEM, MTTI, MTTD, MTTR, управління кіберінцидентами, реагування на інциденти, виявлення інцидентів, автоматизація, моніторинг подій, час реагування, чат-бот, ChatOps, веб-сервери, аналіз трафіку.
Keywords: SIEM, MTTI, MTTD, MTTR, cybersecurity incident management, incident response, incident detection, automatization, event monitoring, response time, chatbot, ChatOps, web-servers, traffic analysis.

СУВЕРЕННІ ХМАРНІ ІНФРАСТРУКТУРИ ЯК ОСНОВА ЦИФРОВОГО СУВЕРЕНІТЕТУ

Чанишев Рашид

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат юридичних наук, доцент

Поняття суверенна хмара (sovereign cloud) з'явилося не так давно. Під цим терміном розуміється створення спеціальної інфраструктури, призначеної для забезпечення відповідності використовуваних у конкретній країні сервісів хмарних обчислень певному набору вимог.

При цьому необхідно враховувати, що сам термін «суверенна хмара» може використовуватися в різних контекстах — як позначення технологічного сервісу, архітектурної або економічної моделі, а також як характеристика певної державної або регіональної політики.

Необхідність створення суверенних хмар обумовлена потребою в забезпеченні контролю над даними, що розміщуються і обробляються в хмарних сервісах, оскільки сама модель хмарних обчислень передбачає зберігання інформації у віддалених центрах обробки даних (ЦОД). При цьому центри обробки даних можуть фізично розташовуватися за межами юрисдикцій держав, в яких знаходяться користувачі відповідних хмарних послуг, що істотно ускладнює їх контроль над інформацією, що зберігається і обробляється в таких центрах.

Наразі більша частина хмарних обчислювальних ресурсів перебуває у власності та під управлінням кількох великих компаній світового рівня, таких як Amazon Web Services, Microsoft Azure та Google Cloud Platform (усі — США, сумарна частка американських компаній на світовому ринку становить 70%). Такі компанії відносять до категорії т.з. глобальних гіперскейлерів (hyperscalers, «гіпермасштабованість»). Ці компанії мають можливість надавати доступ до хмарних ресурсів практично в необмежених обсягах завдяки наявності безлічі великих центрів обробки даних, розподілених по всьому світу, а також за рахунок використання апаратних і програмних технологій власної розробки. Гіперскейлери здатні масштабувати свою інфраструктуру до рівнів, недосяжних для звичайних постачальників хмарних послуг. Саме гіперскейлери формують основу глобального ринку хмарних сервісів і забезпечують роботу більшості цифрових платформ, сервісів і додатків.

Оскільки діяльність гіперскейлерів регулюється законодавством тих країн, в яких вони зареєстровані (а це насамперед США), існує ризик того, що державні органи цих країн можуть у будь-який момент отримати доступ до будь-яких даних в ЦОД на підставі свого власного національного законодавства (наприклад, таких законів, як американський CLOUD Act - Федерального закону США, прийнятого в 2018 році, який регулює порядок

отримання американськими правоохоронними органами доступу до даних, що зберігаються у постачальників хмарних послуг, незалежно від того, чи знаходяться ці дані на території США або за її межами).

CLOUD Act має екстериторіальну дію і може мати пріоритет над місцевими законами про захист даних, якщо запитувана інформація пов'язана з кримінальним розслідуванням, що зачіпає інтереси США. Його положення застосовуються незалежно від фізичного місцезнаходження даних, за умови, що постачальник хмарних послуг зареєстрований у США або здійснює діяльність у правовому полі Сполучених Штатів. Цей Закон надає американській владі право отримати доступ до персональних, корпоративних і навіть конфіденційних даних на підставі судового ордера, причому без обов'язкового повідомлення зацікавлених користувачів або регулюючих органів інших країн [1].

Однак це докорінно суперечить законодавству інших країн. Наприклад, стаття 48 Загального регламенту ЄС щодо захисту персональних даних (GDPR) визначає, що судові розпорядження або вимоги державних органів третіх країн (наприклад, США) можуть бути визнані дійсними в ЄС тільки за наявності відповідної міжнародної угоди, такої як Договір про взаємну правову допомогу (MLAT) [2].

Однак закон CLOUD Act фактично обходить механізм MLAT, надаючи американським властям можливість безпосередньо запитувати дані у компаній, що підпадають під юрисдикцію США, незалежно від того, де фізично знаходяться дані і чи передбачені такі запити міжнародними угодами.

Правова невизначеність, що виникає в такій ситуації, прямо зачіпає питання цифрового суверенітету, оскільки не дозволяє однозначно визначити, правові норми якої юрисдикції — національної чи іноземної — регулюють можливість доступу до даних, що зберігаються у глобальних хмарних провайдерів.

Саме ця правова колізія стала одним із ключових факторів формування концепції «суверенних хмар», що дозволяє визначити та розробити механізми контролю над доступом до даних та їх використанням.

У звіті британської аналітичної компанії Omdia «Omdia Market Radar: Sovereign Cloud 2025» представлена шестирівнева модель можливих реалізацій концепції «суверенної хмари» [3].

Рівень 1 — «Data Residency» (вимога до територіального розміщення даних). На цьому рівні передбачається зобов'язання провайдера хмарних послуг забезпечувати зберігання даних виключно в дата-центрах, розташованих на території відповідної країни. При цьому оперативне управління інфраструктурою та ключовими сервісами може повністю залишатися у віданні зовнішнього постачальника.

Рівень 2 — «Data Processing» (вимога обробки даних всередині національної юрисдикції). На цьому рівні передбачається обов'язкове виконання всіх операцій з обробки даних в межах юрисдикції конкретної держави, що дозволяє знизити ризики несанкціонованого доступу або втручання з боку інших держав. При цьому управління платформою і частиною інфраструктурних процесів все ще може залишатися у віданні зовнішнього постачальника.

Рівень 3 — «Data Privacy» (контроль доступу до даних і захист від зовнішнього втручання). На цьому рівні вимоги суверенітету виходять за рамки фізичного розміщення та обробки даних і включають забезпечення суворих механізмів захисту конфіденційності. Хмарний провайдер зобов'язаний гарантувати, що доступ до даних може здійснюватися виключно уповноваженими суб'єктами, які знаходяться в межах відповідної юрисдикції.

Рівень 4 — «Generated Data Access & Control» або «Cloud Resiliency» (доступ і контроль над створюваними даними та стійкість хмари). На цьому рівні суверенність охоплює не тільки вихідні дані, але й похідні дані, що генеруються в процесі роботи хмарних сервісів: такі, наприклад, як журнали подій, метадані, системні логи, дані аналітики, дані моніторингу, телеметрії та інші дані, пов'язані з експлуатацією та адмініструванням хмарного середовища.

Рівень 5 — «Cloud as Critical Infrastructure» (хмара як критична інфраструктура). На цьому рівні хмарна платформа розглядається як елемент критичної інформаційної інфраструктури держави, нарівні з енергетичними, транспортними, фінансовими та комунікаційними системами. Внаслідок цього до хмари висуваються підвищені вимоги в частині безпеки, стійкості, управління та відповідності національному законодавству.

Рівень 6 — «Self-sufficient Cloud» або «Operational Jurisdiction» (повний операційний суверенітет, контроль ланцюгів поставок та експлуатація на рівні держави). Цей рівень являє собою максимальний ступінь суверенітету хмарної інфраструктури, при якому держава отримує повний контроль над усіма аспектами роботи хмари — від апаратних компонентів до експлуатаційних процесів і оперативного управління.

В рамках запущеної в 2019 році франко-німецької ініціативи GAIA-X AISBL було покладено початок побудові федеративної хмарної інфраструктури ЄС. [4]

За даними звіту Omdia, на даний час позиція, яку займає суверенна хмара ЄС, відповідає лише 3 рівню («Data Privacy») даної моделі. При цьому реалізації повноцінної суверенної хмари в ЄС перешкоджає висока фрагментарність нормативного середовища безлічі держав, що входять до нього.

Однак справжній цифровий суверенітет не може бути забезпечений, поки управління даними залишається у постачальників. Формальне перенесення зберігання даних в ЦОД, територіально розташованих в країнах ЄС, не усуває юридичних ризиків і проблеми безпеки даних, створюючи лише видимість контролю. Справжній суверенітет даних може бути досягнутий лише при використанні власної європейської інфраструктури, доповненої використанням шифрування даних на стороні клієнта, використанням відкритого програмного забезпечення і моделей нульової довіри. Тільки такий комплекс заходів дозволить гарантувати захист даних і створити повноцінне суверенне хмара.

Список використаних джерел

1. OpenCloud. US law in European data centres? The CLOUD Act makes it possible. [Електронний ресурс]. URL: https://opencloud.eu/en/the-cloud-act-makes-it-possible (дата звернення: 10.11.2025).
2. Art. 48 GDPR: Transfers or disclosures not authorised by Union law. [Електронний ресурс]. URL: https://gdpr-info.eu/art-48-gdpr/ (дата звернення: 10.11.2025).
3. Навігація в майбутньому цифрового суверенітету. Omdia Market Radar: Sovereign Cloud 2025. [Електронний ресурс]. URL: https://discover.vultr.com/omdia-sovereign-cloud-2025 (дата звернення: 11.11.2025).
4. Чанишев Р.І. Федеративна європейська інфраструктура даних Gaia-X як інструмент технологічного суверенітету Європи: досвід для України. *Системи та технології*. 2022. №2 (64). С. 48-55. DOI https://doi.org/10.32782/2521-6643-2022.2-64.6/.
5. European Cloud services operate in a largely fragmented environment that poses major challenges in terms of complexity, performance and security [Електронний ресурс]. URL: https://surl.li/kwwbph (дата звернення: 11.11.2025).

Ключові слова: sovereign cloud, цифровий суверенітет, юрисдикція даних, гіперскейлери, моделі можливих реалізацій концепції «суверенної хмари», досвід побудови суверенного хмарного сервісу в ЄС.
Keywords: sovereign cloud, digital sovereignty, data jurisdiction, hyperscalers, models of possible implementations of the “sovereign cloud” concept, experience in building a sovereign cloud service in the EU.

ГРАФОВІ МОДЕЛІ ДЛЯ ВАЛІДАЦІЇ ВРАЗЛИВОСТЕЙ

Денисюк Владислав
Національний технічний університет «Харківський Політехнічний Інститут», аспірант кафедри кібербезпеки

Традиційні методи виявлення та валідації вразливостей – статичний аналіз, динамічне тестування, сканування забезпечують лише локальний погляд на безпеку інформаційної системи. Вони визначають наявність

окремих вразливостей, але не здатні врахувати складні залежності між компонентами, шляхи потенційної експлуатації та каскадний вплив на інші елементи інфраструктури.
У сучасних гібридних та розподілених системах критичним стає **не лише знайти вразливість**, а й **оцінити, як вона може бути використана у ланцюгу атаки**, яким чином взаємодіє з іншими загрозами та чи може спричинити компрометацію системи на вищому рівні. Графові моделі, графи атак, графи залежностей, поведінкові графи дозволяють побудувати комплексне представлення структури системи, її взаємозв'язків, потенційних шляхів експлуатації та ризиків. Вони дають змогу перейти від точкової валідації вразливостей до **системного, структурного та прогнозного аналізу**, що підвищує ефективність валідації [1].

Попри наявність окремих підходів до моделювання шляхів атак, досі бракує адаптивних інтегрованих методів, які одночасно враховували б топологію системи, взаємозв'язки між її компонентами, характеристики вразливостей, ймовірність їх експлуатації та можливості машинного навчання для прогнозування ризику. Це створює потребу у розробці графових моделей, здатних забезпечити ефективну валідацію вразливостей шляхом поєднання аналізу статичних залежностей із урахуванням динамічної поведінки інформаційної системи.

Метою роботи є обґрунтування використання графових моделей для валідації вразливостей у сучасних інформаційних системах, включно з побудовою графів атак, графів залежностей та застосуванням графових методів машинного навчання для оцінки ризику й прогнозування експлуатації.

Графова модель валідації вразливостей може бути формально описана як орієнтований граф:

$$G = (V, E) \qquad (1)$$

де V – це множина вузлів, що відповідають станам системи, компонентам, конфігураціям або вразливостям, а E – це множина орієнтованих ребер, які описують можливі переходи між станами, залежності між компонентами або кроки потенційної атаки. Таким чином, граф надає структурне уявлення про те, як одна вразливість або зміна стану може впливати на інші елементи інформаційної системи. Кожен вузол $v \in V$може мати власні властивості, які характеризують рівень небезпеки чи важливості елемента. Для формального опису їх можна представити у вигляді функції ознак:

$$f(v) \in R^k \qquad (2)$$

де k – це кількість параметрів, наприклад складність експлуатації, критичність компонента або рівень привілеїв, який може бути отриманий при успішній атаці. Ребра графа описують не лише сам факт залежності між вузлами, але й силу або значущість цього зв'язку, що формалізується наступною ваговою функцією:

$$w: E \rightarrow R \geq 0 \qquad (3)$$

У сукупності ці елементи дозволяють досліджувати як статичні властивості системи, так і її динамічну поведінку, моделюючи можливі сценарії розвитку атаки та визначаючи критичні точки, в яких необхідна валідація. Для випадків, коли граф використовується у моделях машинного навчання, застосовується спрощене представлення через матрицю суміжності:

$$A = [a_{ij}] \qquad (4)$$

Де a_{ij} = 1 , якщо між вузлами існує зв'язок, та 0 у протилежному разі. Ознаки вузлів описуються матрицею:

$$X \in R^{Vk} \qquad (5)$$

що використовується як вхід для алгоритмів, здатних враховувати структуру графа при оцінці ризику [2]. Таке формальне представлення дозволяє описати вразливості не як ізольовані об'єкти, а як частини складної системи з численними залежностями, що суттєво підвищує точність і корисність валідації. Графові моделі забезпечують можливість визначати найкоротші шляхи атаки, оцінювати каскадні ефекти та розуміти, як змінюється ризик при додаванні або усуненні певної вразливості. Завдяки цьому вони створюють основу для побудови адаптивних і масштабованих систем валідації, здатних ефективно реагувати на сучасні типи загроз [3]. У цьому контексті графові згорткові мережі (GCN) дозволяють моделі враховувати інформацію сусідніх вузлів, а методи на кшталт GraphSAGE забезпечують ефективність у великій інфраструктурі завдяки семплінгу локальних підграфів. Мережі з механізмами уваги, такі як GAT, здатні визначати найважливіші зв'язки для оцінки ризику та пріоритизації. На відміну від традиційних табличних моделей машинного навчання, які оперують переважно числовими показниками на зразок CVSS, CWE чи KEV, графові методи беруть до уваги структуру зв'язків між компонентами, що робить їх суттєво точнішими та більш придатними для реальних інформаційних систем.

Висновок: у роботі обґрунтовано важливість застосування графових моделей для валідації вразливостей у сучасних інформаційних системах. Графи атак і залежностей дозволяють моделювати комплексні шляхи експлуатації та визначати структурно критичні вразливості. Перспективи подальших досліджень передбачають розробку гібридних моделей, які поєднують графові методи машинного навчання, а також застосування графових нейронних мереж для прогнозування zero-day вразливостей. Подальший розвиток цієї тематики може охоплювати інтеграцію графових моделей у системи типу SIEM та SOAR, а також створення механізмів автоматизованої побудови графів у масштабних інфраструктурах. Важливим напрямом є й формування практичних індикаторів компрометації, побудованих на основі шляхів атаки, що забезпечує більш глибоке та контекстне виявлення загроз.

Список використаної літератури:

1. Angel, D. Protection of Medical Information Systems Against Cyber Attacks: A Graph Theoretical Approach. Wireless Personal Communications, 126, pp. 3455-3464 (2022).
2. A Compact Vulnerability Knowledge Graph for Risk Assessment / J. Yin et al. ACM Transactions on Knowledge Discovery from Data. 2024.
3. Saulaiman M. N.-E., Kozlovszky M., Csilling A. Graph-Based Automation of Threat Analysis and Risk Assessment for Automotive Security. Information. 2025. Vol. 16, no. 6. P. 449.

Ключові слова: графи атак; графи залежностей; валідація вразливостей; графові методи машинного навчання; кібербезпека; моделювання атак; оцінка ризику; експлуатованість; структурний аналіз систем.
Keywords: attack graphs; dependency graphs; vulnerability validation; graph-based machine learning methods; cybersecurity; attack modeling; risk assessment; exploitability; structural system analysis.

AI-ПІДСИЛЕНА ВЕРИФІКАЦІЯ АВТОРСТВА МУЛЬТИМЕДІЙНИХ ДАНИХ В УМОВАХ ГЕНЕРАТИВНОГО ШІ

Овчинников Микола

асистент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Стрімкий розвиток генеративних моделей (GAN, дифузійні моделі) суттєво знизив поріг створення синтетичних зображень, відео та аудіо, що практично не відрізняються від реальних. Це підсилює ризики підміни авторства, масового піратського копіювання, а також формування фальсифікованих доказів у кіберінцидентах. Аналітичні огляди deepfake-атак підкреслюють, що змагальність між генераторами й детекторами призводить до швидкого «старіння» ознак і потребує комбінованих підходів до перевірки достовірності медіа [1,2].

Для задач захисту інтелектуальної власності на мультимедійні дані доцільно переходити від разових перевірок до системної доказовості: фіксації первинного походження, контролю версій, відстеження похідних копій та формування технічно коректного ланцюга збереження (chain of custody). У межах дисертаційної тематики пропонується інформаційна система, що поєднує AI-аналіз контенту, робастне маркування та незмінний журнал подій як основу для доведення авторства та цілісності.

Сучасні атаки на медіа здатні одночасно змінювати семантику (підміна облич, голосу, контексту), маскувати сліди обробки (перекомпресія, ресемплінг, повторне кодування) та обходити детектори через зсув домену або спеціально підібрані збурення. Систематичний огляд методів детекції

показує, що стабільність якості виявлення залежить від різноманітності навчальних даних, коректної валідації й контролю умов застосування [3].

AI-вузол у системі виконує дві взаємодоповнювальні функції: (1) побудова перцептивних «відбитків» (embeddings/хешів) для масштабованого пошуку схожих копій (у тому числі змінених або фрагментованих), (2) оцінка ймовірності синтетичного походження або маніпуляції (детектори фейків, аналіз артефактів, узгодженість метаданих). Така комбінація зменшує залежність від одного індикатора та підвищує відтворюваність результатів перевірки [2,3].

Компонент глибинного watermarking розглядається як механізм маркування, здатний зберігати витягуваність водяного знака після типових перетворень (JPEG/HEVC-компресія, масштабування, кадрування) та частини навмисних атак. Оглядові дослідження підкреслюють, що нейромережеві схеми можуть підвищити робастність і водночас зберегти непомітність, але потребують строгого тестування на різних класах атак і контролю помилок першого/другого роду [4].

Перцептивне хешування доповнює watermarking: навіть якщо знак знищено або істотно спотворено, схожість за перцептивним хешем дозволяє знаходити похідні копії та прив'язувати їх до первинного еталона. В оглядах з перцептивного хешування акцентується компроміс між чутливістю до підробок і стійкістю до допустимих перетворень, а також необхідність ефективної індексації (LSH/ANN) для пошуку в великих колекціях [5].

Узагальнену відповідність типових атак і практичних контрзаходів, які можуть реалізовуватися в AI-підсиленій системі підтвердження авторства, наведено у табл. 1.

Таблиця 1. Узагальнення загроз і контрзаходів для підтвердження авторства мультимедіа. Джерело: авторська розробка.

Загроза (приклад)	**AI/технічний контрзахід**	**Артефакт доказовості**
Підміна авторства / підробка первинних даних	Watermark + перцептивний відбиток; реєстрація хешів	Хеш еталона, watermark-ID, запис реєстрації
Deepfake/синтетична генерація, семантична підміна	Детектори маніпуляцій + порівняння embeddings	Скоринг, різниця embeddings, протокол перевірки
Компресія/масштабування/ кадрування, повторне кодування	Робастне витягування watermark; стійкі хеші	Результат витягування, стійкий хеш, журнал
Стирання watermark, adversarial збурення	Ансамбль детекторів; тест на стійкість; пороги	Метрики/пороги, підтвердження стійкості
Масове копіювання/репости, часткові фрагменти	ANN/LSH пошук за відбитками; виявлення фрагментів	Список збігів, оцінка схожості, джерела

Як видно з табл. 1, для реальних сценаріїв необхідне багатоканальне підтвердження: одночасне використання watermarking, перцептивних відбитків та протоколювання результатів перевірки. Це дозволяє зменшити вплив доменних зсувів для детекторів і зберегти відтворюваність процедури навіть тоді, коли один з каналів частково деградує.

На рис. 1 подано узагальнену архітектуру AI-підсиленої системи захисту авторських прав на мультимедійні дані, у якій поєднуються зазначені механізми.

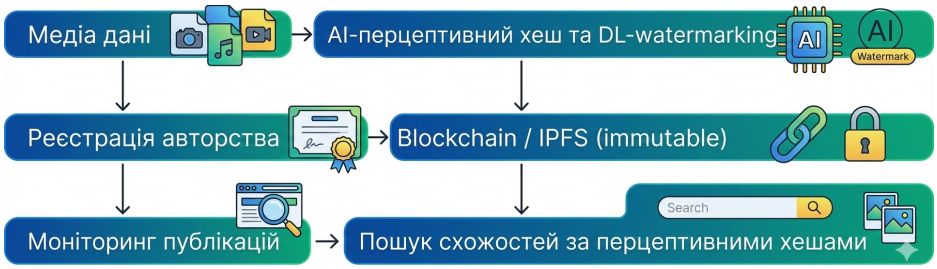

Рис. 1. Архітектура AI-підсиленого захисту авторських прав на мультимедійні дані. Джерело: авторська розробка.

Отже, застосування ШІ в системах захисту авторських прав на мультимедіа доцільно розглядати не як «єдиний детектор», а як складову багатокомпонентного конвеєра, де результат підтверджується незалежними каналами: watermark, перцептивними відбитками та протоколюванням перевірок. Така побудова підвищує стійкість до еволюції генеративних моделей, забезпечує відтворюваність та формує основу для технічно коректного доведення авторства й цілісності у кіберпросторі [1-5].

Список використаних джерел:

1. Tolosana R. et al. Deepfakes and beyond: A survey of face manipulation and fake detection. Information Fusion. 2020;64:131-148. doi:10.1016/j.inffus.2020.06.014.
2. Verdoliva L. Media Forensics and DeepFakes: An Overview. IEEE J. Sel. Top. Signal Process. 2020;14(5):910-932. doi:10.1109/JSTSP.2020.3002101.
3. Rana M.S. et al. Deepfake Detection: A Systematic Literature Review. IEEE Access. 2022;10:25494-25513. doi:10.1109/ACCESS.2022.3154404.
4. Hosny K.M. et al. Digital image watermarking using deep learning: A survey. Computer Science Review. 2024;53:100662. doi:10.1016/j.cosrev.2024.100662.
5. Du L., Ho A.T.S., Cong R. Perceptual hashing for image authentication: A survey. Signal Process.: Image Commun. 2020;81:115713. doi:10.1016/j.image.2019.115713.

Ключові слова: генеративний ШІ, deepfake, мультимедійні дані, цифрове водяне маркування, перцептивне хешування, верифікація авторства, контент-автентифікація, ланцюг доказовості.

Keywords: generative AI, deepfake, multimedia data, digital watermarking, perceptual hashing, authorship verification, content authentication, evidential chain.

Науковий керівник: к.т.н., доцент Ахмаметьєва Г.В.

САМОВДОСКОНАЛЮВАНІ ВІРУСИ ШТУЧНОГО ІНТЕЛЕКТУ: РИЗИКИ, ВИЯВЛЕННЯ ТА МЕТОДИ ПРОТИДІЇ

Лавренко Дмитро

студент факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Штучний інтелект (ШІ) перетворився на подвійний інструмент сучасної кіберзлочинності, де генеративні моделі застосовуються для створення персоналізованих фішингових кампаній, реалістичних deepfake-медіа та імітації людської поведінки з метою обходу систем безпеки. Europol у звіті 2023 року фіксує стрімке зростання злочинів, де ШІ відіграє ключову роль у фальсифікації цифрових доказів, автоматизованому хакінгу та підтримці багатовекторних атак [1]. Це формує технологічне підґрунтя для появи принципово нового класу загроз – самовдосконалюваних шкідливих агентів, здатних адаптувати власну поведінку без прямого втручання оператора.

Під самовдосконалюваними вірусами ШІ розуміють шкідливі програмні агенти з механізмами машинного навчання та адаптації, що дозволяють змінювати стратегії дій, генерувати нові інструкції або модифікувати структуру коду в процесі виконання. Розвиток трансформерних архітектур з механізмами self-attention [2], методів навчання з підкріпленням та еволюційних алгоритмів створює технічні передумови для таких систем. Хоча масових випадків повністю автономних самовдосконалюваних вірусів у відкритому середовищі ще не зафіксовано, задокументовані прототипи демонструють життєздатність цієї парадигми. Зокрема, шкідлива програма PromptLock, проаналізована ESET, застосовувала локально розгорнуту мовну модель для генерації payload-ів у реальному часі, адаптуючи команди до специфіки цільової системи без попередньо захардкоженої логіки атаки [3]. Google Threat Intelligence Group документує зростання кампаній із застосуванням генеративних моделей для варіації шкідливого коду та обходу сигнатурних детекторів [4].

Механізми самовдосконалення реалізуються через трансформерні архітектури, які аналізують контекст і генерують контекстуально оптимізовані інструкції, через навчання з підкріпленням, де дії з високою «винагородою» (успішна ексфільтрація, обхід захисту) підвищують ймовірність повторення подібних стратегій, або через еволюційні алгоритми з мутацією та селекцією варіантів коду на основі метрик ефективності. Найнебезпечнішим є сценарій онлайн-навчання у продуктивному середовищі, коли модель змінює параметри під час виконання, чим ускладнює відтворення її поведінки. Реалізація таких агентів вимагає вибору між локальним розгортанням моделей, що підвищує автономність але обмежене ресурсами, та

використанням віддалених C2-сервісів із потужнішими моделями, що створює виявлювані мережеві індикатори.

Динамічний характер поведінки самовдосконалюваних агентів робить традиційні сигнатурні системи детекції неефективними. Протидія має базуватися на поведінковому аналізі з моделюванням нормальної активності системи та виявленням аномалій у багатовимірному просторі метрик (CPU/IO навантаження, мережеві патерни, частота викликів ML-моделей). Моніторинг інференсу через аналіз нетипового використання ресурсів для inference та кореляція подій у часі можуть виявляти сліди діяльності агента. Sandbox-аналітика має ускладнитись включенням еволюційного тестування: симуляцією різних конфігурацій середовища, імітацією захисних реакцій та відслідковуванням мутацій у стратегіях поведінки.

Наслідки виникнення самовдосконалюваних вірусів є багатовимірними. Технічно це означає зниження ефективності класичних методів виявлення та збільшення часу невиявленої компрометації через варіативність коду. Інфраструктурно підвищується вразливість промислових систем SCADA, енергомереж та транспорту, де адаптивний агент може специфікувати атаки під характеристики обладнання. Економічно прогнозується суттєве здешевлення складних багатоетапних атак через автоматизацію та зростання витрат на постійний захист. Стратегічно виникає потенціал автономної кіберзброї з низьким рівнем людського контролю, що може призводити до незворотних наслідків у критичних сценаріях.

Ефективна протидія вимагає поєднання технічних, організаційних та нормативних заходів. Технічні інструменти включають розширений моніторинг інференсу моделей, виявлення отруєння даних (data poisoning) та контроль доступу до моделей і тренувальних наборів. Організаційні заходи охоплюють політики обмеження запуску неверифікованих моделей у продуктивних середовищах, впровадження принципів Zero Trust та регулярний аудит ML-інфраструктури через SIEM-рішення для кореляції подій. На нормативному рівні необхідні правила автономності моделей, вимоги до сертифікації для критичних застосувань та механізми міжнародного обміну даними про інциденти.

Самовдосконалювані віруси ШІ є реальною науково-технічною загрозою, технічні передумови якої вже створені. Протидія вимагає системної трансформації підходів до кіберзахисту через перехід від сигнатурних методів до поведінкової детекції, інструментування інференсу, захист тренувальних даних та введення нормативних обмежень на автономність моделей. Без цього поширення самонавчальних шкідливих агентів може кардинально змінити ландшафт кіберзлочинності та посилити ризики для критичної інфраструктури й суспільної безпеки.

Список використаних джерел:

1. AI bias in law enforcement. *Europol*. 27.07.2025. URL: https://www.europol.europa.eu/publications-events/publications/ai-bias-in-law-enforcement
2. Vaswani A., Shazeer N., Parmar N., Uszkoreit J., Jones L., Gomez A. N., Kaiser Ł., Polosukhin I. Attention is all you need. *Advances in Neural Information Processing Systems*. 2017. Vol. 30. P. 5998–6008. URL: https://proceedings.neurips.cc/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-Abstract.html
3. ESET discovers PromptLock, the first AI-powered ransomware. *ESET Research.* 27.08.2025. URL: https://www.eset.com/us/about/newsroom/research/eset-discovers-promptlock-the-first-ai-powered-ransomware .
4. GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools. *Google Threat Intelligence Group.* 6.11.2025. URL: https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools/

Ключові слова: самовдосконалювані віруси, штучний інтелект, ШІ, трансформерні архітектури.
Keywords: self-improving viruses, artificial intelligence, AI, transformative architectures.

Науковий керівник: к.т.н., доцент Трофименко О.Г.

МАШИННЕ НАВЧАННЯ У ПЕРЕВІРЦІ ПРОГРАМНИХ КОДІВ: ЕФЕКТИВНІСТЬ АЛГОРИТМУ RANDOM FOREST

Григор'єв Олександр

студент 2 курсу магістратури факультету кібербезпеки та інформаційних технологій Національний університет «Одеська юридична академія»

Перевірка лабораторних робіт з програмування є складним завданням для викладачів, оскільки вимагає великих зусиль як у плані часу, так і когнітивних витрат. Використання методів машинного навчання (МН) дозволяє створити інтелектуальну систему, яка може автоматизувати аналіз програмного коду, виявляти помилки та оцінювати стиль програмування. Для цього рекомендується використовувати алгоритм Random Forest, який поєднує високу точність класифікації з прийнятною швидкістю роботи, забезпечує можливість інтерпретації результатів та виявляє високу стійкість до шумових даних.

Алгоритм Random Forest – це метод машинного навчання, який використовує незалежні дерева рішень, побудовані на основі навчальної вибірки з відомими класами. Кожне дерево навчається на випадковій підмножині даних, враховуючи лише деякі ознаки при формуванні вузлів. Узагальнене рішення моделі визначається шляхом голосування дерев для класифікації або усереднення їхніх прогнозів для регресії [1].

Вибір алгоритму Random Forest для задачі автоматизованої перевірки програмного коду обумовлений низкою переваг. В процесі аналізу програмного коду, використовуються чотири категорії ознак: лексичні, синтаксичні, семантичні та поведінкові. Даний алгоритм ефективно обробляє такі неоднорідні дані без необхідності їх нормалізації або стандартизації, на відміну від багатьох інших алгоритмів машинного навчання. Алгоритм Random Forest дозволяє визначити важливість кожної ознаки, що надає можливість аналізу того, які характеристики коду найбільше впливають на кінцевий результат оцінювання. Це особливо важливо у контексті навчального процесу, де пояснюваність моделі сприяє об'єктивності оцінки та дозволяє викладачам зрозуміти логіку прийняття рішень системою.

Лабораторні роботи здобувачів можуть містити як незначні синтаксичні помилки, так і логічні неточності. Завдяки ансамблевій природі Random Forest є менш чутливим до таких відхилень, ніж окремі класифікатори (наприклад, окреме дерево рішень або логістична регресія).

Модель може бути легко розпаралелена, що забезпечує швидку обробку великої кількості робіт навіть за умови збільшення обсягу даних. Це дозволяє ефективно використовувати метод у реальних умовах, коли система обробляє роботи групи з 25–30 студентів.

Основні параметри моделі (кількість дерев n_estimators, глибина дерева max_depth, мінімальна кількість зразків у листі min_samples_leaf) дозволяють збалансувати точність і швидкодію системи відповідно до конкретних вимог навчального закладу.

Модель для автоматизованої перевірки лабораторних робіт побудована за принципом послідовного конвеєра (pipeline), що поєднує етапи попередньої обробки коду, його векторизації та класифікації результатів.

На початковому етапі здійснюється очищення програмного коду від коментарів, уніфікація імен змінних і функцій, а також нормалізація форматування. Така обробка дає змогу усунути вплив несуттєвих відмінностей у стилі програмування та зосередитися на структурі й логіці реалізації алгоритму.

Векторизація коду перетворює програмний код у числове представлення за допомогою методу TF-IDF (Term Frequency – Inverse Document Frequency [2]), який визначає вагомість кожного токена в межах усієї вибірки. Це дозволяє моделі виокремлювати найважливіші елементи синтаксичної структури програм і враховувати частотні закономірності, характерні для різних типів рішень.

Отримані вектори ознак передаються до класифікаційної моделі, побудованої на основі визначеного алгоритму, який формує ансамбль дерев рішень, де кожне дерево приймає власне рішення, а підсумковий результат

визначається за принципом більшості голосів. Такий підхід забезпечує стійкість моделі до шумових даних і зменшує ризик перенавчання.

Модель інтегрується у процес перевірки робіт у вигляді конвеєра, реалізованого засобами бібліотеки Scikit-learn мовою програмування Python.

Ефективність роботи моделі Random Forest залежить від правильного налаштування її параметрів:

n_estimators (кількість дерев у лісі) – показує кількість дерев рішень, що входять до складу ансамблю. Збільшення кількості дерев підвищує точність моделі, але збільшує час навчання та обсяг використовуваної пам'яті.

max_depth (максимальна глибина дерева) – обмежує глибину кожного дерева. Значення None дозволяє дереву розгалужуватися до повного поділу даних, що забезпечує максимальну точність за умови достатнього обсягу тренувальних даних.

min_samples_split (мінімальна кількість зразків для поділу вузла) – визначає мінімальну кількість зразків, необхідних для поділу внутрішнього вузла. Більші значення запобігають перенавчанню.

max_features (кількість ознак при поділі) – визначає кількість ознак, що розглядаються при кожному поділі. Зазвичай задається як квадратний корінь із загальної кількості ознак.

random_state – фіксується для забезпечення відтворюваності результатів при повторних запусках моделі.

Оптимальні значення параметрів визначаються за допомогою методів пошук за сіткою або випадковий пошук, що дозволяє знайти найкращий баланс між точністю моделі та її обчислювальною ефективністю.

Пошук за сіткою (Grid Search) працює за допомогою сітки значень гіперпараметрів і для кожної комбінації навчається модель та вона оцінюється на основі даних перевірки. У цьому підходу перевіряється кожна окрема комбінація значень гіперпараметрів, що може бути дуже неефективно.

Випадковий пошук (Randomized Search) – створюється сітка значень гіперпараметрів та обирається випадкові комбінації для навчання моделі та оцінювання. Кількість ітерацій пошуку встановлюється на основі часу/ресурсів [3].

Перевагами використання алгоритму Random Forest для створення та навчання моделі є висока точність класифікації – модель поєднує результати багатьох незалежних дерев рішень, що забезпечує точність на рівні 85-92%. Стійкість до неповних даних – алгоритм ефективно працює навіть у випадку перевірки робіт здобувачів, які можуть містити помилки або відмінності в стилі програмування. Оцінювання важливості ознак – можливість визначити, які характеристики коду найбільше впливають на підсумкову оцінку, що підвищує інтерпретованість результатів. Масштабованість – модель легко розпаралелюється та може працювати в паралельному режимі, що

робить її придатною для аналізу великих обсягів даних. Простота використання – не потребує складного налаштування параметрів для досягнення стабільної якості класифікації.

Отже, використання алгоритму Random Forest у поєднанні з TF-IDF-представленням коду забезпечує збалансоване поєднання високої точності, стійкості до варіативності студентських рішень і достатньої прозорості оцінювання. Це робить обраний підхід ефективним інструментом для реалізації інтелектуальної системи автоматизованої перевірки лабораторних робіт з програмування мовою Python.

Список використаних джерел:

1. Random Forest, Explained: A Visual Guide with Code Examples. URL: https://surl.li/usfdoz (дата звернення: 10.11.2025)
2. Understanding TF-IDF (Term Frequency-Inverse Document Frequency). URL: https://surl.li/ouyept (дата звернення: 10.11.2025)
3. Intro to Model Tuning: Grid and Random Search. URL: https://surl.li/ygdymi (дата звернення: 10.11.2025)

Ключові слова: машинне навчання, алгоритм, інтелектуальна система, Random Forest
Keyword: machine learning, algorithm, intelligent system, Random Forest

Науковий керівник: доц. Логінова Н.І.

ІНТЕРНЕТ РЕЧЕЙ (IOT) ЯК ІНСТРУМЕНТ БІЗНЕС-МЕНЕДЖМЕНТУ

Літовченко Данило

студент 1 курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Інтернет речей, або Internet of Things (IoT), перетворився на одну з ключових технологій, що формує новий тип управлінської логіки в бізнесі. У центрі цієї концепції лежить взаємодія фізичних об’єктів через мережу, що дає змогу збирати, передавати та аналізувати дані в режимі реального часу. Таке середовище даних створює нові можливості для бізнес-менеджменту, в якому швидкість прийняття рішень, точність прогнозування та оперативна адаптація стають критично важливими [1].

Сучасні компанії інтегрують IoT для оптимізації виробництва, логістики, контролю якості, автоматизації управління ресурсами та формування інтелектуальних продуктів і сервісів. Таким чином, IoT стає фундаментальним елементом цифрової трансформації й рушійною силою конкурентних переваг у глобальній економіці [2].

Даний звіт досліджує сутність IoT, механізми його роботи та ключові напрями застосування у бізнес-менеджменті. Аналіз охоплює можливості, ризики, переваги та перспективи подальшого розвитку IoT як інструменту управління. Особлива увага приділяється практичним прикладам, що демонструють реальну цінність технології для управлінських процесів.

Архітектура IoT базується на з'єднанні фізичних пристроїв через інтернет або локальні мережі, утворюючи багаторівневу систему. Основу складають сенсори, контролери, мережеві протоколи та хмарні платформи, які забезпечують збір, передобробку та аналіз даних. Кожен фізичний об'єкт виступає вузлом даних, передаючи інформацію в аналітичні платформи. Такі дані дозволяють керівникам виявляти приховані закономірності, контролювати навантаження на обладнання, прогнозувати несправності та підвищувати точність управлінських рішень [3].

Функціонування IoT забезпечується сучасними бездротовими технологіями: Wi-Fi, Bluetooth Low Energy, Narrowband IoT, LTE-M і 5G. Поява 5G особливо важлива, оскільки вона дає високу пропускну здатність, мінімальні затримки та можливість одночасного підключення великої кількості пристроїв. Це робить IoT придатним для складних корпоративних інфраструктур та промислових середовищ [4].

IoT значно підсилює ефективність операційних процесів. Сенсорні системи контролюють виробниче обладнання, аналізують технічний стан, прогнозують поломки та дозволяють автоматизувати технічне обслуговування. Такий підхід мінімізує простої, скорочує витрати та збільшує продуктивність. IoT переводить управління у стан, де рішення приймаються на основі фактичних даних, а не припущень, що суттєво підвищує точність управління [5].

Концепція прозорої логістичної інфраструктури також формується за допомогою IoT. Використання RFID-міток, GPS-трекерів, датчиків температури та систем моніторингу забезпечує доступ до даних про рух товару в реальному часі. Це дозволяє оптимізувати маршрути транспортування, уникати псування продукції, прогнозувати затримки та раціонально розподіляти складські ресурси. Управління ланцюгами постачання стає точним, що позитивно впливає на прибутковість бізнесу [6].

Аналітика є ключовим елементом IoT у бізнесі. Технологія створює великий потік даних, які обробляються за допомогою машинного навчання, статистичних моделей та штучного інтелекту. Компанії можуть прогнозувати попит, моделювати поведінку споживачів, виявляти відхилення у роботі систем і точніше планувати діяльність. IoT фактично формує нову культуру менеджменту, засновану на даних, а не на інтуїції.

Активне застосування IoT також стосується взаємодії зі споживачами. Розумні пристрої збирають дані про поведінку клієнтів, відстежують їхні

переваги й дозволяють створювати персоналізовані пропозиції. Це формує модель випереджальної клієнтської підтримки, у якій компанія передбачає потребу до того, як клієнт її висловить. Таким чином, IoT виступає основу для побудови лояльності й індивідуалізованого сервісу.

Незважаючи на значні переваги, IoT супроводжується суттєвими викликами. Одним із центральних є інформаційна безпека: велика кількість підключених пристроїв створює значну поверхню атаки, ускладнює сегментацію мережі, оновлення прошивок і управління правами доступу [7].

Додатково існують питання конфіденційності персональних даних, сумісності обладнання, високої вартості впровадження та інтеграції із застарілими системами. Бізнес має розробляти комплексні стратегії захисту та впроваджувати кібербезпекові стандарти для мінімізації ризиків.

Очікується масштабне зростання IoT-рішень у корпоративному секторі протягом найближчих років. Технологія стає доступнішою, швидшою та інтелектуальнішою. Поширення 5G, розвиток хмарних платформ та поява нових сенсорів сприятимуть розширенню IoT у виробництві, транспорті, фінансах, медицині та сфері обслуговування. IoT стає не просто інструментом, а базовою інфраструктурою бізнесу.

Новий аспект полягає у впровадженні IoT у межах інтегрованого управління процесами підприємства (Business Process Management). Об'єднання IoT і BPM дозволяє створити адаптивні ланцюги процесів, які автоматично реагують на зміни контексту та внутрішнього стану системи. Це відкриває шлях до автономізації управлінських рішень і структурної оптимізації бізнес-операцій [8].

Другим важливим напрямом розвитку є екологічний і соціальний вплив IoT. Підприємства впроваджують рішення для моніторингу енерговитрат, викидів, якості довкілля і стану інфраструктури; це дозволяє керівництву підвищувати екологічну відповідальність та звітування відповідно до міжнародних стандартів сталого розвитку. Таким чином, IoT стає інструментом не лише управлінського, але й стратегічного характеру.

Назагал, Інтернет речей є одним із найважливіших інструментів менеджменту в сучасному бізнесі. Його застосування охоплює оптимізацію виробництва, покращення логістики, цифрову аналітику, формування клієнтоорієнтованих стратегій та створення інтелектуальних бізнес-моделей. Компанії, які впроваджують IoT-технології, отримують конкурентні переваги, знижують витрати та підвищують якість управління. Незважаючи на супутні ризики, IoT стає ключовою технологією економіки даних.

Список використаних джерел

1. Sevak K.Y. "The evolution of Internet of Things (IoT) research in business and management." Journal of Information Technology & Digital Economy. 2024. URL:

https://www.emerald.com/jide/article/4/3/242/1212329/The-evolution-of-Internet-of-Things-IoT-research [дата звернення: 06.11.2025]
2. IoT in Business Management: Opportunities, Challenges and Future Implications. ResearchGate. 2023. URL: https://www.researchgate.net/publication/370952972_IoT_in_Business_Management_Opportunities_Challenges_and_Future_Implications [дата звернення: 06.11.2025]
3. The Role of the Internet of Things (IoT) in Business and ... Atlantis Press. 2021. URL: https://www.atlantis-press.com/article/125960576.pdf [дата звернення: 06.11.2025]
4. Applications for the Internet of Things (IoT) in business. Nexford Insights. 2025. URL: https://www.nexford.edu/insights/applications-for-the-internet-of-things-iot-in-business [дата звернення: 06.11.2025]
5. Internet of Things: Impact on business. InovaDigital. 2022. URL: https://www.inovadigital.eu/en/internet-of-things-impact-on-business/ [дата звернення: 06.11.2025]
6. How IoT has Impacted Business Operations. PXP Blog. URL: https://pxp.io/blog/iot-in-business-operations [дата звернення: 06.11.2025]
7. Nearly half of network connections come from high-risk IoT and IT devices – TechRadar. (2025) URL: https://www.techradar.com/pro/security/nearly-half-of-network-connections-come-from-high-risk-iot-and-it-devices-so-make-sure-youre-protected [дата звернення: 06.11.2025]
8. On the Interplay Between Business Process Management and IoT. Business & Information Systems Engineering. 2024. URL: https://link.springer.com/article/10.1007/s12599-024-00859-6 [дата звернення: 06.11.2025]

Ключові слова: Інтернет речей; цифрова трансформація; аналітика бізнес-даних; логістика й виробництво; кібербезпека пристроїв.
Keywords: Internet of Things; digital transformation; business data analytics; logistics and manufacturing; IoT cybersecurity.

Науковий керівник: к.ю.н. доцент Чанишев Р.І.

МЕТОДИ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЗНАЧЕННЯ СТИЛІВ НАВЧАННЯ

Дашдаміров Гліб

студент 2 курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Моделі машинного навчання (МН) відкривають нові можливості для виявлення прихованих закономірностей у поведінці здобувачів освіти, їхніх взаємодіях з навчальним контентом, темпах засвоєння матеріалу та когнітивних патернах. Використання таких моделей дозволяє не лише класифікувати стилі навчання (візуальний, аудіальний тощо), а й прогнозувати ефективність освітніх стратегій, адаптувати контент у реальному часі та підвищувати мотивацію здобувачів.

Актуальність дослідження зумовлена широким впровадженням цифрових освітніх платформ, де МН може бути інтегроване для аналізу поведінкових даних. А також зростанням обсягів освітніх даних, що потребують інтелектуальної обробки та потребою в адаптивних системах навчання, які враховують індивідуальні особливості здобувачів.

Отже, розробка моделі машинного навчання для визначення стилів навчання є актуальним напрямом дослідження, що поєднує інноваційні технології з педагогічною практикою, сприяючи розвитку адаптивних освітніх систем нового покоління.

У межах адаптивних систем навчання задача визначення стилю навчання може трактуватися по-різному. Якщо доступні дані з наперед визначеними мітками стилів, проблему формулюють як класифікацію, де модель навчається за супервізованим підходом. У ситуації, коли такої розмітки немає, застосовують методи кластеризації, які дозволяють виявити приховані групи поведінкових патернів без попередніх припущень. Вибір між цими двома підходами залежить від структури доступної вибірки та наявності міток.

Для класифікаційних задач зазвичай застосовують алгоритм Random Forest, який поєднує багато дерев рішень і забезпечує високу точність та стійкість до перенавчання [1]. Також використовують алгоритм Support Vector Machine (SVM), що добре працює з даними високої розмірності та чітко визначеними межами між класами [2] або штучні нейронні мережі, що здатні моделювати складні нелінійні залежності та ефективні на великих наборах даних [3].

Якщо ж модель має виконувати кластеризацію, часто використовують K-means, який швидко знаходить групи за умови попереднього вибору їх кількості [4], або DBSCAN, що дозволяє будувати кластери довільної форми та виявляти шумові дані [5].

Побудова моделі потребує використання ознак, які відображають реальну поведінку користувача в освітньому середовищі. Йдеться про час взаємодії з різними типами контенту, послідовність його дій у системі, результати початкових тестів, характерні помилки, а також особливості навігації, такі як глибина перегляду навчальних модулів чи частота повернення до вже пройдених матеріалів. Сукупність цих характеристик формує вектор ознак, що подається на вхід моделі.

У випадку використання нейронної мережі структура зазвичай включає вхідний шар із кількістю нейронів, що відповідає обсягу нормалізованих даних, кілька прихованих шарів із функцією активації ReLU та регуляризацією Dropout для запобігання перенавчанню, а також вихідний шар, який формує або ймовірності належності до певного стилю (через Softmax), або векторне

представлення даних, якщо мережу застосовують у контексті кластеризації [6].

Алгоритми МН вимагають налаштування гіперпараметрів: у випадку Random Forest це стосується кількості дерев і їхньої максимальної глибини. Для SVM - вибору ядра, параметра регуляризації та оптимізації через крос-валідацію. Для K-means - визначення кількості кластерів за допомогою методу «лікоть» чи силуетного аналізу. Для DBSCAN - підбору значень ε та мінімального числа точок.

Оцінювання якості моделі проводять за допомогою метрик точності, повноти, F1-міри та аналізу матриці помилок, що дозволяє зрозуміти, які стилі плутаються між собою. Для кластеризаційних моделей застосовують коефіцієнт силуету, індекс Девіса–Боулдіна або скоригований індекс Ренда, якщо еталонна розмітка все ж доступна.

Таким чином, моделі МН забезпечують комплексний підхід до визначення стилів навчання, сприяючи розвитку адаптивних навчальних систем нового покоління.

Список використаних джерел:

1. Random Forest Algorithm Overview. H. A. Salman, A. Kalakech, & A. Steiti , Trans. *Babylonian Journal of Machine Learning*, *2024*, 69-79. https://doi.org/10.58496/BJML/2024/007
2. Support Vector Machines: Types of SVM. URL: https://www.upgrad.com/blog/support-vector-machines (дата звернення: 7.11.2025).
3. Yousif, J. H., Yousif, M. J. Critical Review of Neural Network Generations and Models Design. Preprints 2023, 2023091149. https://doi.org/10.20944/preprints202309.1149.v2.
4. K-Means Clustering Algorithm. URL: https://www.analyticsvidhya.com/blog/2019/08/comprehensive-guide-k-means-clustering (дата звернення 1.11.2025)
5. A Guide to the DBSCAN Clustering Algorithm. URL: https://www.datacamp.com/tutorial/dbscan-clustering-algorithm (дата звернення 1.11.2025)
6. Neural Network Model. URL: https://www.sciencedirect.com/topics/computer-science/neural-network-model (дата звернення 2.11.2025)

Ключові слова: машинне навчання,
Keyword: machine learning,

Науковий керівник: доц. Логінова Н.І.

КОНТРОЛЬ ЦІЛІСНОСТІ БАЗИ ДАНИХ ЗА ДОПОМОГОЮ БЛОКЧЕЙНІВ

Бойко Віктор

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат технічних наук

Панчук Ганна

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Найважливішою умовою для новітніх інформаційних систем є дотримання достовірності даних, якщо цілісність масивів буде порушена, присутня велика можливість втратити точність даних, ускладнити процедури точності даних, аналізу та мати фінансові втрати. Такі стандарти як, запис всіх операцій, обчислення контрольних сум, резервування, є дієвими, коли присутня повна довіра до людей, які керують системою та відсутні будь які ризики з довірою [1].

Метод блокчейну, у свою чергу, дає інший підхід, який гарантує недоторканість інформації. Його суть полягає у формуванні послідовного реєстру транзакцій, де кожен блок містить у собі хеш попереднього. Через такий спосіб, спроба змінити остаточну інформацію дуже важко та одразу виявляється, оскільки порушується взаємозв'язок усіх елементів цього ланцюга [2].

Блокчейн є переліком блоків, де кожен містить у собі інформацію та хеш попереднього блоку. Для забезпечення надійності та незмінності інформації застосовується такий алгоритм :

– Хешування записів – кожне внесення змін або додавання елемента до бази даних супроводжується генеруванням хешу.

– Формування блоку – сформований набір хешів об'єднується в один блок. Об'єднаний блок отримує тимчасову мітку, а саме ідентифікатор користувача, який здійснив дію, яка, у свою чергу, посилається на попередній блок у ланцюгу.

– Запис у блокчейн-реєстр – Виконується пересилання створеного блоку до розподіленого або гібридного блокчейн-мережі, яка зберігається окрема від первинної бази даних.

– Підтвердження – система повторно обчислює хеші для поточних даних і звіряє їх з тими, що були зафіксовані у блокчейні. У разі виявлення невідповідностей відбувається фіксація порушення цілісності. [3, 4]

Перевагами такої системи є:

– Гарантія незмінності записів – після того, як користувач затвердив блок у ланцюга, будь-яка спроба модифікації буде виявлено акт втручання.

– Розподілений механізм контролю – відбувається мінімізація загроз будь-яких маніпуляцій, це відбувається через відсутність єдиного центру зберігання даних.

– Мінімальне використання ресурсів – система може працювати як додатковий рівень поверх існуючих систем керування базами даних, це не вимагає значні обчислювальні ресурси.

– Спрощене впровадження – можлива реалізація через стандартизовані програмні інтерфейси без потреби створення повноцінного публічного блокчейну.

– Прозорість аудиту – кожен запис даних може бути незалежно перевірений сторонами [2, 4].

Створимо порівняльну таблицю, яка надасть нам бачення ефективності порівняно з традиційними методами контролю, та проставимо бали від 0 до 5, де 0 – найнижча оцінка, 5 – найвища.

Таблиця 1 Порівняння методів контролю

Метод контролю	Виявлення втручання	Рівень захисту	Прозорість аудиту	Вимоги ресурсів
Блокчейн	5	5	4	3
Журналювання транзакцій	4	3	3	4
Контроль сум	2	3	3	2
Резервне копіювання	4	3	2	5

Отже, можемо побачити, що блокчейн забезпечує найвищий рівень захисту при низькому споживання ресурсів [3, 1].

Подальші напрями розвитку охоплюють поєднання технологій блокчейну зі штучним інтелектом для автоматичного виявлення аномалій у транзакціях, а також з квантово-стійкими алгоритмами шифрування, які можуть гарантувати безпеку в умовах квантових обчислень [3].

Одним із перспективних рішень є також створення хмарних блокчейн-сервісів, що надають змогу організаціям інтегрувати контроль цілісності у свої бази даних без великих витрат.

Одним із прикладів є застосування контролю цілісності бази даних за допомогою блокчейнів у сфері фінансів. Він може бути застосований для підтвердження достовірності транзакцій у бухгалтерських реєстрах. Кожна фінансова операція отримує свій запис у блокчейні та має свою унікальну мітку. Якщо хтось спробує змінити, додати або вилучити запис у базі даних, відповідний хеш не збігатиметься з початковими даними в реєстрі, що дозволяє миттєво виявити спробу шахрайства [1, 5].

Впровадження блокчейнів для контролю цілісності баз даних забезпечує найвищий рівень захисту при мінімальних ресурсних витратах. Даний підхід дає змогу виявляти спроби втручання даних у реальному часі та створює надійну основу для побудови довірених цифрових систем. Застосування такого методу є значним у сферах, де критично важливим є збереження автентичності записів, наприклад банківської, юридичної, методичної сфер.

Список використаних джерел:

1. Кузьменко О. В. Методи забезпечення цілісності інформації в розподілених базах даних. – К.: НТУУ КПІ, 2020.
2. Соловйов А. В. *Криптографічні методи захисту інформації*. – Харків: Університет внутрішніх справ, 2018.
3. Antonopoulos A. M. *Mastering Blockchain*. – O'Reilly Media, 2021.
4. Chen L., Xu L., Shah N., Gao Z., Lu Y., Shi W. On Security Analysis of Proof-of-Work and Proof-of-Stake in Blockchain. – IEEE Transactions, 2019.
5. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. – 2008.

Ключові слова: Блокчейн, Контроль цілісності, База даних, Розподілений реєстр, Хешування, Незмінність записів, Прозорість аудиту, Виявлення втручання.
Keywords: Blockchain, Integrity Control, Database, Distributed Ledger, Hashing, Immutability of Records, Audit Transparency, Tampering Detection.

ОГЛЯД ЕВОЛЮЦІЇ АРХІТЕКТУРИ ІГРОВИХ РУШІЇВ

Толокнов Анатолій
асистент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»

Ігрові рушії становлять технологічну основу сучасної індустрії відеоігор, надаючи розробникам комплексні інструменти для побудови інтерактивних віртуальних просторів. Протягом останніх років архітектурна організація ігрових рушіїв зазнала суттєвих перетворень, переходячи від монолітних структур до модульних, високоефективних систем [1]. Провідні представники галузі, Unity та Unreal Engine, продовжують встановлювати індустріальні стандарти, проте паралельно з'являються спеціалізовані платформи, розроблені для специфічних жанрів та технічних вимог.

Архітектурний розвиток ігрових рушіїв пройшов тривалий шлях від елементарних двовимірних систем до комплексних багатокомпонентних платформ. Традиційна об'єктно-орієнтована архітектура, що тривалий час домінувала в галузі, поступово замінюється більш ефективними підходами, зокрема Entity Component System (ECS) [2]. Архітектура ECS представляє

фундаментальну зміну парадигми в організації ігрової логіки. На відміну від класичної ієрархії успадкування, ECS розділяє дані (компоненти) та поведінку (системи), що значно покращує продуктивність завдяки оптимізованій локальності даних у пам'яті [2]. Сутності виступають лише як унікальні ідентифікатори, які об'єднують компоненти, тоді як системи обробляють ці компоненти масово, забезпечуючи паралельну обробку та ефективне використання процесорного кешу.

Unity впровадив власний підхід до ECS через Data-Oriented Technology Stack (DOTS), який включає Job System для багатопоточності та Burst Compiler для оптимізації коду. Unreal Engine також рухається в цьому напрямку з системою Mass для обробки великомасштабних симуляцій [2]. Ці архітектурні трансформації відображають загальну тенденцію індустрії до підвищення продуктивності та масштабованості систем.

Графічний конвеєр залишається одним з найбільш критичних компонентів ігрового рушія. Процес перетворення тривимірних моделей у двовимірні зображення включає декілька ключових етапів: обробку геометрії, растеризацію, затінення та освітлення, пост-обробку та композицію кадру [3]. Unreal Engine традиційно використовує відкладений рендеринг (deferred rendering), що дозволяє обробляти складні сцени з великою кількістю джерел світла [3]. Революційні технології Unreal Engine 5, Nanite та Lumen, визначають новий стандарт якості графіки. Nanite забезпечує віртуалізовану геометрію з мільярдами полігонів без необхідності ручного створення рівнів деталізації. Lumen пропонує повністю динамічне глобальне освітлення в реальному часі, що усуває потребу в попередньому запіканні світла.

Unity надає розробникам більшу гнучкість через три окремі конвеєри рендерингу: вбудований (Built-In), Universal Render Pipeline (URP) для мобільних платформ та VR, і High Definition Render Pipeline (HDRP) для високоякісної графіки AAA-рівня [3]. URP використовує прямий рендеринг (forward rendering), що забезпечує кращу продуктивність на менш потужному обладнанні, тоді як HDRP пропонує фізично-коректний рендеринг, об'ємне освітлення та трасування променів у реальному часі [3].

Процес рендерингу включає декілька критичних стадій оптимізації. Відсікання (culling) видаляє об'єкти поза полем зору камери, система рівнів деталізації (LOD) автоматично знижує складність віддалених об'єктів, а батчинг об'єднує декілька об'єктів для зменшення кількості викликів відрисовки [4]. Сучасні рушії також активно використовують асинхронні обчислення, дозволяючи паралельну обробку різних стадій конвеєру.

Фізичні рушії відповідають за симуляцію реалістичної поведінки об'єктів у віртуальному світі. Unity використовує NVIDIA PhysX, тоді як Unreal Engine має власну інтегровану фізичну систему з розширеними можливостями для

складної балістики та взаємодій [5]. Оптимізація фізики є критично важливою для підтримки стабільної частоти кадрів.

Ключові техніки включають просторове розбиття (spatial partitioning) для зменшення кількості перевірок колізій, використання простих колайдерів замість складних мешів, та систему «сну» об'єктів (object sleeping) для деактивації фізики статичних тіл. Асинхронні фізичні обчислення дозволяють виконувати симуляцію в окремому потоці, звільняючи основний потік для інших завдань. Сучасні рушії також впроваджують шарову систему колізій та масок для точного контролю над тим, які об'єкти можуть взаємодіяти один з одним, що значно зменшує обчислювальне навантаження. Для мобільних платформ особливо важливою є оптимізація фізичного тайм-степу та використання фіксованого оновлення для забезпечення передбачуваної поведінки.

Паралельно з розвитком універсальних рушіїв спостерігається зростання спеціалізованих рішень, орієнтованих на конкретні жанри або платформи. CryEngine зарекомендував себе як оптимальний вибір для фізично-орієнтованих шутерів від першої особи з реалістичною балістикою [5]. Godot завоював популярність серед інді-розробників завдяки відкритому вихідному коду та ефективній роботі з двовимірними іграми [5].

Bevy Engine представляє нове покоління рушіїв, побудованих на мові Rust з повною інтеграцією ECS з самого початку. Його архітектура забезпечує масивно паралельну та кеш-дружню обробку даних, що робить його привабливим для проектів, де продуктивність є критичною. Flax Engine пропонує високоякісну тривимірну графіку з підтримкою численних платформ і вбудованими онлайн-сервісами.

Спеціалізація також відбувається на рівні створення контенту. З'являються вертикальні платформи для конкретних жанрів, такі як інструменти для створення Battle Royale або ARPG-ігор. Ці рішення забезпечують більш глибоку інтеграцію специфічних для жанру механік та оптимізацій, дозволяючи розробникам швидше створювати якісний контент.

Інтеграція штучного інтелекту стає невід'ємною частиною архітектури сучасних ігрових рушіїв. AI використовується не лише для поведінки NPC, але й для процедурної генерації контенту (PCG), автоматизованого тестування та оптимізації продуктивності. Процедурна генерація дозволяє створювати величезні ігрові світи, рівні та навіть персонажів автоматично, значно зменшуючи ручну роботу розробників.

Unity ML-Agents Toolkit надає інструменти для навчання інтелектуальних агентів через машинне навчання, а Unreal Engine інтегрує Behavior Trees та AI Perception для створення реалістичної поведінки NPC. Майбутні рушії обіцяють хмарну розробку з повною інтеграцією AI-інструментів для створення контенту в реальному часі. Це відкриває нові можливості для динамічного сторітелінгу,

де наратив адаптується до дій гравця, створюючи унікальний досвід кожного проходження.

Архітектура ігрових рушіїв переживає період інтенсивної трансформації, рухаючись від монолітних об'єктно-орієнтованих систем до модульних, data-oriented рішень з акцентом на продуктивність та масштабованість [1]. Unity та Unreal Engine продовжують лідирувати, впроваджуючи революційні технології, такі як DOTS, Nanite та Lumen, але спеціалізовані рушії знаходять свою нішу, пропонуючи оптимізовані рішення для конкретних завдань [5].

Майбутнє ігрових рушіїв лежить у площині глибшої інтеграції штучного інтелекту, розвитку хмарних технологій та подальшої спеціалізації під конкретні жанри та платформи [1]. Архітектура ECS стає стандартом де-факто для високопродуктивних систем [2], а процедурна генерація відкриває нові горизонти для створення унікального контенту. Ці тренди визначатимуть розвиток індустрії найближчими роками, роблячи розробку ігор більш доступною та ефективною.

Список використаних джерел

1. Unity vs Unreal Engine's Latest Features: 2025 Q1 overlook. Pingle Studio. 2025. URL: https://pinglestudio.com/blog/unity-vs-unreal-engines-latest-features-2024-q1-overlook (дата звернення: 2.11.2025).
2. Entity-Component-System (ECS) Architecture in Game Development. Daydream Soft. 2025. URL: https://www.daydreamsoft.com/blog/mastering-entity-component-system-ecs-in-game-development (дата звернення: 4.11.2025).
3. How Game Engines Like Unreal Engine and Unity Handle 3D Rendering. iRendering. 2025. URL: https://irendering.net/how-game-engines-like-unreal-engine-and-unity-handle-3d-rendering/ (дата звернення: 4.11.2025).
4. Understanding the Rendering Pipeline: Essentials for Traditional and Real-Time Rendering. Garage Farm. 2024. URL: https://garagefarm.net/blog/understanding-the-rendering-pipeline-essentials-for-traditional-and-real-time-rendering (дата звернення: 8.11.2025).
5. Unity vs Unreal: A Detailed Performance Showdown. Pingle Studio. 2024. URL: https://pinglestudio.com/blog/unity-vs-unreal-a-detailed-performance-showdown (дата звернення: 10.11.2025).

Ключові слова: ігрові рушії, архітектура ігор, Entity Component System (ECS), Data-Oriented Technology Stack (DOTS), рендеринг, графічні конвеєри, фізичні рушії, оптимізація продуктивності, процедурна генерація контенту, штучний інтелект у іграх, спеціалізовані рушії, мультиплатформеність, Nanite, Lumen, Unity, Unreal Engine.

Keywords: game engines, game architecture, Entity Component System (ECS), Data-Oriented Technology Stack (DOTS), rendering, graphics pipelines, physics engines, performance optimization, procedural content generation, artificial intelligence in games, specialized engines, cross-platform, Nanite, Lumen, Unity, Unreal Engine.

БЛОКЧЕЙН-ТЕХНОЛОГІЇ В ЗАБЕЗПЕЧЕННІ ЦІЛІСНОСТІ ДАНИХ

Соловйов Артем

Національний університет «Одеська юридична академія», асистент кафедри інформаційних технологій

Цілісність даних є критично важливим аспектом інформаційної безпеки, що гарантує незмінність, точність та достовірність інформації протягом усього її життєвого циклу. У сучасному цифровому світі, де обсяги даних зростають експоненційно, а кіберзагрози стають дедалі складнішими, традиційні методи забезпечення цілісності даних виявляються недостатньо надійними.

Блокчейн-технологія, вперше представлена як основа криптовалюти Bitcoin у 2008 році, пропонує революційний підхід до вирішення проблеми цілісності даних. Завдяки своїй децентралізованій архітектурі, криптографічним механізмам та консенсусним алгоритмам, блокчейн створює незмінний та прозорий реєстр транзакцій, який практично неможливо підробити або модифікувати без виявлення.

Мета дослідження: проаналізувати технічні механізми блокчейн-технології, що забезпечують цілісність даних, та дослідити практичні застосування цих механізмів у сфері кібербезпеки.

Актуальність теми обумовлена зростаючою потребою організацій у надійних механізмах захисту критичних даних від несанкціонованих змін, а також необхідністю створення довірчих систем в умовах відсутності централізованих органів контролю.

1. Технічні основи блокчейн-технології

1.1. Архітектура блокчейну

Блокчейн являє собою розподілену базу даних, що складається з ланцюжка блоків, кожен з яких містить набір транзакцій. Кожен блок включає:

- Заголовок блоку: містить метадані, включаючи хеш попереднього блоку, мітку часу, nonce та корінь дерева Меркла
- Тіло блоку: містить список транзакцій
- Криптографічний хеш: унікальний ідентифікатор блоку, обчислений на основі всіх його даних

Ключовою особливістю є те, що кожен блок містить хеш попереднього блоку, створюючи незламний криптографічний ланцюжок. Будь-яка спроба модифікувати дані в одному блоці призведе до зміни його хешу, що автоматично інвалідує всі наступні блоки.

1.2. Криптографічні механізми забезпечення цілісності

Хеш-функції є фундаментальним інструментом забезпечення цілісності в блокчейні. Найчастіше використовуються SHA-256 (в Bitcoin) та Keccak-256 (в Ethereum). Ці функції мають наступні властивості:

- Детермінованість: однакові вхідні дані завжди дають однаковий хеш
- Односторонність: практично неможливо відновити вхідні дані з хешу
- Ефект лавини: навіть мінімальна зміна вхідних даних кардинально змінює хеш
- Стійкість до колізій: практично неможливо знайти два різні входи з однаковим хешем [1].

2. Механізми забезпечення цілісності даних

2.1. Незмінність історичних записів

Найважливіша властивість блокчейну для цілісності даних - це практична незмінність історичних записів. Якщо зловмисник намагається змінити дані в блоці, який знаходиться на глибині N блоків від кінця ланцюжка:

1. Зміна даних в блоці призводить до зміни його хешу
2. Це вимагає перерахунку хешу наступного блоку, який містить хеш модифікованого блоку
3. Процес каскадно поширюється на всі наступні N блоків
4. Зловмисник повинен перерахувати всі ці блоки швидше, ніж чесні вузли додають нові блоки

При використанні PoW це вимагає контролю над >51% обчислювальної потужності мережі, що економічно недоцільно для великих публічних блокчейнів. Для Bitcoin, наприклад, вартість такої атаки оцінюється в мільярди доларів [2].

3. Практичні застосування в кібербезпеці

3.1. Управління ланцюжками постачання

Блокчейн забезпечує цілісність даних про походження та переміщення товарів:

- IBM Food Trust: відстежує продукти харчування від ферми до магазину, дозволяючи швидко ідентифікувати джерело контамінації
- Everledger: реєструє походження діамантів для боротьби з конфліктними діамантами
- VeChain: перевіряє автентичність розкішних товарів та фармацевтичних препаратів

Криптографічні хеші фізичних товарів реєструються в блокчейні, створюючи незмінний audit trail.

3.2. Управління цифровими ідентичностями

Децентралізовані системи ідентичності використовують блокчейн для:

- Створення самосуверенних цифрових ідентичностей, контрольованих користувачем
- Захисту від підробки документів та крадіжки особистих даних
- Забезпечення цілісності верифікаційних даних (освітніх сертифікатів, дипломів, ліцензій)

Приклади: Civic, uPort, Sovrin Foundation.

3.3. Захист цілісності логів та аудитів

Критичні системні логи можуть зберігатися в блокчейні або анкоритися до блокчейну через регулярне публікування хешів:

- Унеможливлює видалення або модифікацію логів зловмисниками після компрометації системи
- Забезпечує судову значимість логів для форензичного аналізу
- Дозволяє виявити момент компрометації шляхом порівняння локальних логів з блокчейн-записами

3.4. Безпека IoT-пристроїв

Блокчейн може вирішити проблеми безпеки Інтернету речей:

- Firmware integrity: хеші затверджених версій firmware зберігаються в блокчейні, пристрої перевіряють цілісність перед оновленням
- Децентралізована автентифікація: пристрої можуть автентифікуватися один перед одним без централізованого сервера
- Незмінний журнал взаємодій: всі комунікації між IoT-пристроями записуються, дозволяючи виявити аномальну поведінку

3.5. Захист інтелектуальної власності

Блокчейн надає timestamp-сервіс для доказу існування документів в певний момент часу:

- Автори можуть анкорити хеші своїх творів в блокчейн, створюючи незаперечний доказ авторства
- Патентні відомства можуть використовувати блокчейн для реєстрації заявок
- Цифрові активи (NFT) підтверджують автентичність та власність цифрових об'єктів

4. Обмеження та виклики

4.1. Масштабованість

Публічні блокчейни мають обмежену пропускну здатність:

- Bitcoin: ~7 транзакцій/секунду
- Ethereum: ~15-30 транзакцій/секунду

Це неприйнятно для додатків, що вимагають високої швидкості обробки. Рішення включають:

- Layer-2 протоколи
- Sharding - розподіл блокчейну на паралельні ланцюжки
- Sidechains та state channels

4.2. Конфіденційність

Прозорість блокчейну може конфліктувати з вимогами конфіденційності. Рішення:

- Zero-knowledge proofs: дозволяють доводити істинність тверджень без розкриття даних
- Приватні блокчейни з контрольованим доступом
- Анкорінг: зберігання лише хешів конфіденційних даних в публічному блокчейні

4.3. Енергоспоживання

PoW-блокчейни споживають величезну кількість електроенергії. Альтернативи:

- Перехід на PoS
- Використання відновлюваних джерел енергії
- Вибір більш ефективних консенсусних механізмів для корпоративних застосувань [3].

Блокчейн-технологія представляє парадигмальний зсув у підходах до забезпечення цілісності даних. Завдяки комбінації криптографічних механізмів, децентралізованої архітектури та консенсусних алгоритмів, блокчейн створює практично незмінний реєстр, який не залежить від довіри до централізованих органів.

Блокчейн не є універсальним рішенням для всіх проблем цілісності даних, але для застосувань, що вимагають децентралізованої довіри, незмінності та прозорості, він представляє одну з найбільш перспективних технологій сучасної кібербезпеки.

Список використаних джерел:

1.Buterin,V.Ethereum White Paper. 2014. URL: https://ethereum.org/en/whitepaper/.

2. Crosby, M. et al. BlockChain Technology: Beyond Bitcoin. Applied Innovation Review. 2016. Issue

2. URL: https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf.

3. Zyskind, G., Nathan, O. Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops. 2015. URL: https://ieeexplore.ieee.org/document/7163223

Ключові слова: Блокчейн, цілісність даних, криптографія, хеш-функції, консенсусні алгоритми, децентралізація, кібербезпека.

Keywords: Blockchain, data integrity, cryptography, hash functions, consensus algorithms, decentralization, cybersecurity.

ІНФОРМАЦІЙНА ГЕОМЕТРІЯ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ТОЧНОСТІ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

Чепурна Олена

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат фізико-математичних наук

Черевко Євген

доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», кандидат фізико-математичних наук

Розвиток систем машинного навчання вимагає дедалі точніших засобів представлення та аналізу структур даних. Одним із таких підходів є інформаційна геометрія, яка оперує поняттями статистичних многовидів, дивергенцій, метричних структур і ріманових метрик для моделювання параметричних просторів розподілів. Її методи дозволяють переходити від класичного евклідового простору до більш придатних для аналізу інформаційних просторів, де зберігається інваріантність до деформацій і логарифмічних масштабувань [1, с. 18].

Центральним об'єктом аналізу є статистичний многовид – гладкий многовид , у якому кожна точка відповідає розподілу ймовірностей , де – вектор параметрів. Визначеною на ньому метрикою є метрика Фішера, яка вводиться як:

$$g_{ij}(\theta) = \mathbb{E}[\frac{\partial \log\ p(x;\theta)}{\partial \theta_i}\frac{\partial \log\ p(x;\theta)}{\partial \theta_j}],$$

де очікування береться відносно $p(x;\theta)$. Така метрика дозволяє визначити геодезичні криві, обчислювати довжини та кути між напрямами зміни параметрів, що уможливлює побудову ефективних алгоритмів градієнтного спуску у задачах навчання [2, с. 142–143].

Іншим важливим поняттям є дивергенція Кульбака–Лейблера:

$$D_{\mathrm{KL}}(p \parallel q) = \int p(x) \log \frac{p(x)}{q(x)} dx,$$

яка відіграє роль функції відстані між двома розподілами, незважаючи на її несиметричність. Геометрична структура, індукована цією дивергенцією, забезпечує можливість оптимізації моделей у задачах класифікації, регресії та виявлення аномалій [3, с. 79].

У сфері кібербезпеки особливої уваги заслуговує застосування інформаційно-геометричних методів до задач виявлення вторгнень (IDS), де ймовірнісні розподіли ознак мережевого трафіку можуть розглядатися як точки на статистичному многовиді. Наприклад, зміна геодезичної відстані між

базовим розподілом нормального трафіку та поточним розподілом може свідчити про відхилення, що наближається до аномального режиму [4, с. 33].

У сучасних підходах дедалі активніше інтегруються методи інформаційної геометрії в алгоритми навчання на багатовимірних даних. Наприклад, у роботі [5, с. 11–22] описані геометричні метрики які можна використовувати як частину механізму оптимізації в багаторівневих моделях. Такі підходи вже знаходять практичне застосування в розподілених інтелектуальних системах, зокрема в енергетичних мережах, де необхідна здатність до адаптивного реагування на аномалії в режимі реального часу [6, с. 9–11].

Додаткову роль у формуванні геометрії статистичного простору відіграє концепція двоїстих зв'язностей (Dual Affine Connections), яка дозволяє моделювати не лише симетричні, а й асиметричні зв'язки між розподілами. Це актуально в системах, де має місце неповна інформація або різнотипні джерела даних (наприклад, кіберфізичні системи з мультисенсорними потоками) [7, с. 213–215].

Нормативний та методологічний контекст також формує запит на використання інформаційної геометрії в системах оцінювання ризиків. У межах структури NIST Cybersecurity Framework 2.0 [8] можуть бути інтегровані геометричні моделі як частина інструментарію для ідентифікації критичних відхилень, зокрема в аналітиці поведінки користувачів та обчислювальних систем.

Водночас українське правове поле, зокрема Закон України «Про основні засади забезпечення кібербезпеки України» [9], визначає принципи захисту інформаційних ресурсів, які можуть бути вдосконалені через використання математично строго обґрунтованих методів виявлення ризиків.

Враховуючи зростаючу складність кіберзагроз та обмеженість класичних статистичних методів при роботі з великомасштабними даними високої розмірності, інформаційна геометрія відкриває нові напрямки для досліджень. Одним із перспективних напрямів є подальше формалізоване вивчення геометрії статистичних многовидів для побудови інваріантних моделей виявлення аномалій у середовищах з нестабільною розподільчою структурою. Зокрема, це стосується OT/ICS-архітектур, розподілених систем контролю та адаптивних систем в енергетичній, транспортній та телекомунікаційній інфраструктурах.

Окремий інтерес становить застосування інформаційно-геометричних моделей у поєднанні з байєсівськими і варіаційними методами для поліпшення стійкості до атак типу Adversarial, що особливо актуально у сфері безпеки автономних систем. Також доцільно розглядати інтеграцію ріманових метрик та геодезичних дивергенцій до структур Explainable AI (XAI), що дозволить інтерпретувати поведінку критичних моделей у кібербезпекових системах.

З практичної точки зору, доцільним є впровадження окремих компонентів інформаційної геометрії у нормативні та методологічні рамки управління ризиками, а також у проєктування процедур виявлення аномалій у системах реагування CERT-типу. Такий підхід дозволить підвищити як точність виявлення інцидентів, так і адаптивність до нових сценаріїв загроз.

Узагальнено використання інформаційної геометрії як структурного підходу в задачах аналізу даних та побудови безпечних систем відкриває простір для міждисциплінарних досліджень, що поєднують кібербезпеку, диференціальну геометрію, статистику та теорію інформації.

Список використаних джерел:

1. Amari S. Information Geometry and Its Applications. Springer. 2016. 381 p. DOI: 10.1007/978-4-431-55978-8.
2. Nielsen F. An Elementary Introduction to Information Geometry. Entropy. 2020. Vol. 22. No. 10. P. 1100. DOI: 10.3390/e22101100.
3. Cover T.M., Thomas J.A. Elements of Information Theory. 2nd ed. Wiley. 2006. 784 p. ISBN: 978-0471241959.
4. Derhab A., Bouras A. Multivariate correlation analysis and geometric linear similarity for real-time intrusion detection systems. Security and Communication Networks. 2015. Vol. 8. No. 4. P. 1193–1212. DOI: 10.1002/sec.1074.
5. Cherevko Y., Chepurna O., Kuleshova Y. On Information Geometry Methods for Data Analysis. Geometry Integrability and Quantization. 2024. Vol. 29. P. 11–22. DOI: 10.7546/giq-29-2024-11-22.
6. Chen Y., Li C., Xu Z. Information Geometry Based Anomaly Detection for Cyber–Physical Systems. IEEE Transactions on Industrial Informatics. 2020. Vol. 16. No. 9. P. 6193–6202. DOI: 10.1109/TII.2019.2952914.
7. Lauritzen S.L. Statistical Manifolds. In: Differential Geometry in Statistical Inference. Institute of Mathematical Statistics. 1987. P. 163–216. DOI: 10.1214/lnms/1215454097.
8. National Institute of Standards and Technology. The NIST Cybersecurity Framework 2.0. 2024. URL: https://www.nist.gov/cyberframework
9. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19

Ключові слова: інформаційна геометрія, статистичні многовиди, геодезичні відстані, Riemann-метрика, виявлення аномалій, машинне навчання, кібербезпека, дивергенція, інтерпретованість моделей, захист критичної інфраструктури

Keywords: information geometry, statistical manifolds, geodesic distance, Riemannian metric, anomaly detection, machine learning, cybersecurity, divergence, model interpretability, critical infrastructure protection

ВРАХУВАННЯ ЕНЕРГОЕФЕКТИВНОСТІ ТА РОБАСТНОСТІ В МОДЕЛЯХ СИСТЕМ КІБЕРБЕЗПЕКИ

Юсипів Андрій

студент кафедри кібербезпеки Західноукраїнського національного університету, м. Тернопіль, Україна

Стійкість інформаційних систем (ІС) – ключова властивість, що забезпечує їхню працездатність за умов кіберзагроз та параметричних збурень. Робастність – характеристика стабільності при варіаціях вхідних умов. Проблема моделювання ІС полягає в інтеграції стійкості, безпеки та енергоефективності в єдину оптимізаційну модель за наявності невизначеності.

У роботі [1] розглянуто нечіткі моделі (на основі математичної моделі нечітких множин – див. [2, 3]) розпізнавання мовлення, стійкі до шумів, що можна адаптувати до аналізу трафіку. Гібридні моделі ANFIS розглядалися в роботі [4], а застосування нечітких множин у задачах управління – у [5]. Перші енергоефективні IoT-системи з моніторингом з'являються у роботі [6]. Проте більшість робіт аналізують ці аспекти ізольовано, без комплексного врахування усіх трьох вимірів.

Мета – розробка гібридної моделі на основі нечітких генетичних алгоритмів (FGA) для одночасної оптимізації безпеки, енергоефективності та робастності.

Виклад основного матеріалу. Виконаємо опис математичної моделі необхідної нам системи. Нехай $X = (x_1, x_2, \dots, x_n) \in R^n$ – вектор параметрів політики безпеки (пороги виявлення, ваги ризиків, тощо). Цільова функція стійкості $f(X)$ тут є багатокритеріальною:

$$f(X) = w_1 S(X) + w_2 E(X) + w_3 R(X),$$

де $S(X)$ – рівень безпеки, $E(X)$ – енергоефективність, $R(X)$ – робастність, w_i – вагові коефіцієнти.

Рівень безпеки моделюється через нечітку систему виведення:

$$S(X) = \sum_{k=1}^{M} \overline{w_k}(p_k x_1 + q_k x_2 + r_k),$$

де $\overline{w_k} = \frac{\mu_{A_k}(x_1)\mu_{B_k}(x_2)}{\sum \mu_{A_i}\mu_{B_i}}$ – нормалізована сила активації правила.

Енергоефективність $E(X) = 1 - \frac{\sum_{i=1}^{n} c_i x_i}{E_{max}}$, де c_i – енергетична вартість.

Робастність $R(X) = \exp\left(-\sum_{i=1}^{n} \left|\frac{\partial f}{\partial x_i}\right| \Delta x_i\right)$.

Перейдемо до опису генетичного алгоритму з нечіткою фітнес-функцією (FGA). Він складається з наступних етапів:

- ініціалізація популяції $P_0 = \{X_1, \dots, X_m\}$;
- оцінка $f_k = \mu_{high}(f(X_k))$, де $\mu_{high}(z) = \frac{1}{1+e^{-k(z-z_0)}}$;

- селекція – турнірна з ймовірністю $p_s = \frac{f_k}{\sum f_i}$;
- кросовер $X' = \alpha X_i + (1-\alpha)X_j,\ \alpha \in [0,1]$;
- мутація $x_l' = x_l + \mathcal{N}\left(0, \sigma \cdot \left(1 - \mu_{robust}(X)\right)\right)$.

Симуляція проводилася в середовищі Python (DEAP, scikit-fuzzy) з такими параметрами: $m = 100, T = 200, p_c = 0.8, p_m = 0.1$. Наступна таблиця ілюструє порівняльний аналіз різних методів.

Методи	Безпека	Енергоефективність	Робастність	Час, с
Традиційні	≤0.72	≤0.65	≤0.68	≤0,1
ANFIS	0.81	0.70	0.74	12,4
FGA (запропон.)	**0.91**	**0.83**	**0.89**	**8,7**

Табл. 1. Порівняльний аналіз методів оптимізації стійкості інформаційних систем.

Висновки. У межах дослідження розроблено гібридну модель FGA, що оптимізує стійкість систем кібербезпеки за трьома критеріями: безпека, енергоефективність, робастність. Модель поєднує нечітку логіку для обробки невизначеності та генетичні алгоритми для глобальної оптимізації. Симуляція підтверджує перевагу FGA над традиційними та нейро-нечіткими методами за точністю, швидкістю та адаптивністю, відкриваючи шлях до нового покоління інтелектуальних систем кібербезпеки.

Список використаних джерел

1. Гуйда О.Г., Юсипів Т.В. Кисельов В.Б., Омецинська Н.В., Курилко О.Б. Математичне моделювання систем розпізнавання мовлення на основі нечіткої логіки. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки*. 2025. Том 36 (75) №3. С. 125-129. DOI: 10.32782/2663-5941/2025.3.1/16.
2. Pedrycz W. Fuzzy systems engineering: Toward human-centric computing. John Wiley & Sons. 2011. 526 p. DOI: 10.1002/9780470168967.
3. Klir G. J., Yuan B. Fuzzy set theory: Foundations and applications. Prentice Hall. 2006. 574 p.
4. Takagi T., Sugeno M. Fuzzy identification of systems and its applications to modeling and control. *IEEE transactions on systems, man, and cybernetics*. 1985. Vol. 15, no. 1. Pp. 116–132.
5. Желдак Т.А., Коряшкіна Л.С., Ус С.А. Нечіткі множини в системах управління та прийняття рішень: навчальний посібник. Дніпро: НТУ «Дніпровська політехніка», 2020. 387 с.
6. Скрипка К.І., Гуйда О.Г., Омецинська Н.В., Лісовець С.М., Юсипів Т.В. Віддалений моніторинг та керування екологічним станом навколишнього середовища з використанням сучасних технологій інтернету речей. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки*. 2023. Том 34 (73) № 3. С. 233-238. DOI: 10.32782/2663-5941/2023.3.1/36.

ІДІОМА RAII ЯК ЕВОЛЮЦІЙНА ВІДПОВІДЬ НА ПРОБЛЕМИ РУЧНОГО УПРАВЛІННЯ ПАМ'ЯТТЮ В C++

Д'якова Ксенія

Національний університет «Одеська юридична академія», студентка факультету кібербезпеки та інформаційних технологій

Мова програмування C++ історично поєднує низькорівневу потужність C із засобами об'єктно-орієнтованого програмування. Однією з її ключових особливостей є прямий контроль над динамічною пам'яттю, що дозволяє створювати високопродуктивні системи, але водночас породжує складні та небезпечні помилки. У ранніх версіях C++ (до C++11) управління пам'яттю здійснювалося вручну – через оператори new та delete, що вимагало від програміста абсолютної дисципліни та точності. Витоки пам'яті, висячі вказівники, подвійне звільнення – ці помилки не лише ускладнювали розробку, а й створювали серйозні ризики для стабільності та безпеки програмного забезпечення [1].

Ручне управління пам'яттю в C++ передбачає, що програміст самостійно відповідає за виділення та звільнення ресурсів. Оператор new створює об'єкт у купі (heap), а delete – знищує його та повертає пам'ять системі. Якщо delete не викликається, виникає витік пам'яті – ресурс залишається захопленим, але недоступним, що поступово призводить до вичерпання доступної пам'яті [2]. Особливо небезпечними є ситуації, коли програма достроково виходить з функції, минаючи виклик delete (рис. 1), або коли вказівник продовжує посилатися на вже звільнену область – так званий висячий вказівник (рис. 2). У першому демонстраційному прикладі показано, як достроковий вихід з функції без виклику delete призводить до витоку пам'яті, а в другому прикладі – доступ до висячого вказівника – програма продовжує працювати, створюючи ілюзію коректності, хоча фактично виконується код з невизначеною поведінкою (Undefined Behavior), що може призвести до краху програми або порушення безпеки. Висячі вказівники перетворюють програму на "мінне поле" невизначеної поведінки. Спроба доступу до звільненої пам'яті може не викликати миттєвої помилки, створюючи ілюзію коректної роботи, але водночас пошкоджуючи дані або створюючи вразливості, які проявляться значно пізніше і в зовсім іншій частині коду. Діагностика таких помилок є одним із найскладніших завдань у програмуванні. Наслідки таких помилок часто не проявляються одразу, що ускладнює їх діагностику.

```
#include <iostream>
#include <string>

// Використовуємо стандартний простір імен для спрощення
```

```
using namespace std;

// 1. Допоміжний клас для демонстрації управління ресурсами
class Resource {
private:
   string name;
public:
   Resource(string n) : name(n) {
      cout << "  [+] RESOURCE '" << name << "' CREATED." << endl;
   }
   ~Resource() {
      cout << "  [-] RESOURCE '" << name << "' DESTROYED." << endl;
   }
   void use() {
      cout << "  [*] Using resource '" << name << "'." << endl;
   }
};

// 2. Функція, що демонструє проблему
void demonstrate_memory_leak(bool condition) {
   cout << "Entering function 'demonstrate_memory_leak'..." << endl;
   Resource* ptr = new Resource("Leaked Resource");

   if (condition) {
      cout << "  Condition is true. Early return!" << endl;
      // ПОМИЛКА: Ми виходимо з функції, не викликавши delete.
      return;
   }

   ptr->use();
   delete ptr;
   cout << "Leaving function 'demonstrate_memory_leak'..." << endl;
}

// 3. Головна функція для запуску
int main() {
   demonstrate_memory_leak(true); // Викликаємо з умовою, що спричиняє витік
   cout << "\nAfter function call. 'Leaked Resource' was never destroyed." << endl;
   return 0;
}
```

Рисунок 1 – Код-приклад "вистріл в ногу"

```
#include <iostream>
#include <string>

// Використовуємо стандартний простір імен для спрощення
using namespace std;

// 1. Той самий допоміжний клас
class Resource {
private:
   string name;
public:
   Resource(string n) : name(n) {
      cout << "  [+] RESOURCE '" << name << "' CREATED." << endl;
   }
```

```
    ~Resource() {
        cout << "  [-] RESOURCE '" << name << "' DESTROYED." << endl;
    }
    void use() {
        cout << "  [*] Using resource '" << name << "'." << endl;
    }
};

// 2. Функція, що демонструє проблему
void demonstrate_dangling_pointer() {
    cout << "\nEntering function 'demonstrate_dangling_pointer'..." << endl;
    Resource* ptr1 = new Resource("Dangling Test");
    Resource* ptr2 = ptr1;

    cout << "  Deleting ptr1..." << endl;
    delete ptr1; // Пам'ять звільнена, деструктор викликано.

    cout << "  Trying to use ptr2..." << endl;
    // КАТАСТРОФА: Доступ до вже звільненої пам'яті.
    ptr2->use();

    cout << "Leaving function 'demonstrate_dangling_pointer'..." << endl;
}

// 3. Головна функція для запуску
int main() {
    demonstrate_dangling_pointer();
    return 0;
}
```

Рисунок 2 – Код для демонстрації висячого вказівника

Саме ці виклики стали рушієм еволюції мови C++ у напрямі безпечного управління ресурсами. Пошук рішення привів до формулювання ідіоми RAII – Resource Acquisition Is Initialization – яка докорінно змінила підхід до роботи з пам’яттю. RAII передбачає, що захоплення ресурсу (наприклад, пам’яті) відбувається в конструкторі об’єкта, а його звільнення – у деструкторі. Це дозволяє прив’язати життєвий цикл ресурсу до життєвого циклу об’єкта. Якщо об’єкт створено на стеку, його деструктор гарантовано викликається при виході з області видимості – незалежно від того, чи це нормальне завершення функції, чи виняткова ситуація [3].

На рис. 3 показано, як створення об’єкта Resource на стеку забезпечує автоматичне звільнення пам’яті без явного виклику delete. Це усуває ризик витоку пам’яті навіть у випадках дострокового виходу з функції або винятків.

```
#include <iostream>
#include <string>

using namespace std;

// Допоміжний клас, що імітує ресурс, який потрібно створювати та знищувати
class Resource {
```

```
public:
    // Конструктор "захоплює" ресурс
    explicit Resource(const string& name) : name_(name) {
        cout << "[+] RESOURCE '" << name_ << "' CREATED." << endl;
    }

    // Деструктор "звільняє" ресурс
    ~Resource() {
        cout << "[-] RESOURCE '" << name_ << "' DESTROYED." << endl;
    }

    void use() const {
        cout << "[*] Using resource '" << name_ << "'." << endl;
    }

private:
    string name_;
};

// Функція, що демонструє автоматичне управління життєвим циклом об'єкта
void demonstrate_raii_on_stack() {
    cout << "\nEntering function 'demonstrate_raii_on_stack'..." << endl;
    {
        cout << "  Entering inner scope..." << endl;
        // 1. Створення об'єкта на стеку
        // Викликається конструктор Resource
        Resource res("Stack-based RAII");

        // 2. Використання ресурсу
        res.use();

        cout << "  Leaving inner scope..." << endl;
        // 3. Вихід з області видимості
        // Деструктор для 'res' викликається автоматично
    }
    cout << "Leaving function 'demonstrate_raii_on_stack'..." << endl;
}

int main() {
    demonstrate_raii_on_stack();
    return 0;
}
```

Рисунок 3 – Демонстрація ідіоми RAII для об'єкта, створеного на стеку

RAII не лише вирішує проблему витоків, а й унеможливлює доступ до звільненої пам’яті, оскільки об’єкт знищується автоматично, і вказівник на нього більше не існує. Це усуває клас помилок, пов’язаних із висячими вказівниками. RAII є фундаментом сучасного C++ і реалізується через стандартні засоби, зокрема, розумні вказівники (std::unique_ptr, std::shared_ptr), які автоматично керують ресурсами. У поєднанні з винятками, шаблонами та контейнерами STL, RAII дозволяє створювати безпечний, надійний та масштабований код [4].

Особливо важливим є застосування RAII у системах, де стабільність і контроль над ресурсами є критичними: розробка ігрових рушіїв, високочастотний трейдинг, системне програмування, вбудовані системи, наукові обчислення. У таких середовищах помилка управління пам’яттю може

призвести до катастрофічних наслідків, тому автоматизація цього процесу є не просто бажаною, а необхідною. Також RAII сприяє покращенню читабельності та підтримуваності коду. Програміст більше не повинен вручну відстежувати, де і коли викликати delete, що зменшує когнітивне навантаження та ризик помилок. Це особливо важливо в командній розробці, де код часто змінюється і доповнюється різними учасниками.

Хоча RAII ідеально працює для об'єктів на стеку, у багатьох задачах потрібне створення об'єктів у динамічній пам'яті, наприклад, при побудові дерев, списків або фабрик об'єктів. У таких випадках RAII реалізується через обгортки – розумні вказівники, які інкапсулюють динамічний ресурс і керують ним автоматично. Це дозволяє поєднати гнучкість динамічної пам'яті з безпекою автоматичного управління.

У сучасному C++ (починаючи з C11) ідіома RAII стала стандартом. Її підтримують всі основні бібліотеки, а нові засоби – такі як std::move, std::make_unique, std::make_shared – роблять її ще зручнішою. Це свідчить про те, що RAII не лише вирішила проблему ручного управління пам'яттю, а й стала основою нової парадигми програмування в C.

Тим самим ідіома RAII є еволюційною відповіддю на фундаментальні проблеми ручного управління пам'яттю в C++. Вона забезпечує автоматичне, безпечне та передбачуване управління ресурсами, усуває ризики витоків пам'яті, висячих вказівників та невизначеної поведінки. RAII стала основою сучасного C++ і є критично важливою для розробки надійного програмного забезпечення в системах з високими вимогами до стабільності та продуктивності.

Список використаних джерел:

1. Stroustrup B. Quotes. *Goodreads*. URL: https://www.goodreads.com/author/quotes/64947.Bjarne_Stroustrup
2. Meyers S. Effective C++: 55 Specific Ways to Improve Your Programs and Designs. Addison-Wesley, 2011. 297 p. URL: https://ptgmedia.pearsoncmg.com/images/9780321334879/samplepages/0321334876.pdf
3. RAII. *cppreference.com*. URL: https://en.cppreference.com/w/cpp/language/raii.html
4. ISO/IEC 14882:2024(E) – Programming Language C++ 23. URL: https://isocpp.org/std/the-standard

Ключові слова: управління пам'яттю, C++, витоки пам'яті, висячі вказівники, ідіома RAII.
Keywords: memory management, C++, memory leaks, dangling pointers, RAII idiom.

Науковий керівник: к.т.н., доцент Трофименко О.Г.

ВИКОРИСТАННЯ МУЛЬТИМЕДІЙНИХ ТЕХНОЛОГІЙ У СТВОРЕННІ СУЧАСНИХ ІГРОВИХ ЗАСТОСУНКІВ

Задерейко Олександр

кандидат технічних наук, доцент кафедри інформаційних технологій факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Корчовий Михайло

студент 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Ігрові застосунки сьогодні є найскладнішими формами мультимедійних систем, у яких поєднуються візуальні, звукові, текстові, сенсорні та інтерактивні компоненти. Мультимедійні технології виступають основою архітектури сучасних ігор, забезпечуючи синтез різних типів даних у цілісний користувацький досвід. Їхня роль полягає не лише у візуалізації, а й у створенні інтерактивного середовища, де кожен елемент — графіка, звук чи анімація — впливає на сприйняття та реакції користувача.

Візуальна складова є центральним елементом мультимедійної інтеграції. Рушії *Unreal Engine 5* та *Unity HDRP* забезпечують підтримку трасування променів (ray tracing), глобального освітлення (*Lumen*), процедурної генерації матеріалів і фізично коректного рендерингу (*Physically Based Rendering*, PBR). Такі технології створюють високу реалістичність, що сприяє повнішому зануренню гравця у середовище. За даними *Hendrikx M. et al., ACM TOMM* (*2011*), використання процедурної графіки скорочує обсяг ручної роботи дизайнерів на 40–60 % і дозволяє досягти більшої варіативності контенту [1].

Сучасні ігрові рушії використовують алгоритми динамічного освітлення, глобального затінення та постобробки — такі як *Ambient Occlusion*, *Bloom*, *Motion Blur*, *Depth of Field*. Ці засоби створюють кінематографічну глибину кадру. Анімаційні системи базуються на методах інверсної кінематики (IK), фізичних симуляцій (*ragdoll physics*), процедурного руху та морфінгу. Взаємодія гравця з середовищем реалізується через *event-driven systems* і *state machines*, які синхронізують анімаційні, звукові та візуальні події в реальному часі.

Звукові технології є ще одним критично важливим аспектом мультимедійного дизайну. Ігрові аудіосистеми реалізують просторове 3D-звучання, динамічне мікшування та параметричне аудіо, яке реагує на дії користувача. Наприклад, рушій *FMOD Studio* або *Wwise* дозволяє пов’язати звуки зі станами об’єктів у грі, створюючи повністю інтерактивне середовище. Згідно з дослідженням *Cambridge University Press* (*2014*), звукові ефекти та музика підвищують рівень залученості користувачів і формують емоційний контекст геймплею, підсилюючи когнітивне сприйняття візуальних сцен.

Інтерактивність є визначальною характеристикою мультимедійних ігор. Вона забезпечує двосторонній зв'язок між системою та користувачем через сенсорні події, контролери, рухові трекери або мікрофони. Сучасні рушії реалізують інтерактивність через подієво-орієнтовану архітектуру, у якій усі мультимедійні елементи синхронізуються зі станами гри. *Journal of Multimedia Technology and Trends* (*2023*) підкреслює, що інтерактивність є ключовим чинником, який формує залучення користувача та перетворює його з пасивного спостерігача на активного учасника процесу [8].

Використання процедурної генерації контенту (*Procedural Content Generation*, PCG) є одним із найбільш ефективних напрямів розвитку мультимедійних систем у геймдизайні. Методи *PCG* дозволяють автоматично створювати рівні, моделі, ландшафти, текстури або навіть сценарії на основі алгоритмів випадковості чи машинного навчання. У роботі *Togelius J. et al., arXiv:1702.00539* (*2017*) зазначається, що використання *PCGML* (Procedural Content Generation Via Machine Learning) дає змогу створювати контент, який адаптується під стиль гравця, тим самим підвищуючи варіативність і реіграбельність гри [2]. Крім того, такі підходи значно скорочують час і ресурси розробки, що є критичним для великих ігрових студій.

Машинне навчання та штучний інтелект відіграють усе більшу роль у формуванні мультимедійного контенту. Системи на основі нейронних мереж здатні створювати динамічні звукові сцени, адаптивні текстури або поведінкові моделі персонажів, які навчаються від користувача. *PURL* (*NSF, 2023*) вказує, що глибоке навчання дає змогу побудувати мультимедійні системи, які аналізують стиль гри користувача та змінюють візуальні й аудіоелементи в реальному часі [3].

XR-технології (VR, AR, MR) стали черговим кроком у розвитку інтерактивного мультимедіа. Віртуальна реальність (VR) поєднує тривимірну графіку, просторове аудіо, сенсорні системи та механізми зворотного зв'язку, формуючи ефект «повної присутності». Згідно з дослідженням *Gunkel S.N.B. et al., arXiv:2201.05552* (*2022*), головним викликом XR-систем є синхронізація мультимедійних потоків для уникнення затримок та артефактів у відображенні [4]. *Wang H., Dong J. et al.* (*2023*) у дослідженні *ACM Digital Library* доводять, що ефективна мультимедійна інтеграція під час XR-стримінгу забезпечує стабільність частоти кадрів і природність руху об'єктів у середовищі [5].

Мультимедіа в ігрових застосунках тісно пов'язана з проблемою оптимізації ресурсів. Сучасні ігри мають обмеження щодо пам'яті, продуктивності процесора та графічних обчислень. Тому активно застосовуються технології *Level of Detail* (*LOD*), динамічне масштабування

текстур, кешування аудіо та асинхронне завантаження об'єктів. За даними *ResearchGate* (*2023*), оптимізація мультимедійних потоків може підвищити продуктивність ігор на 25–35 % без втрати якості [6].

Значний розвиток мультимедійних технологій відбувається і в напрямі *serious games* — навчальних, медичних та тренувальних симуляторів. За даними *Springer* (*2012*), використання інтерактивних мультимедійних елементів у таких іграх підвищує рівень засвоєння матеріалу на 30–40 % завдяки ефекту поєднання когнітивних та сенсорних каналів сприйняття [7]. Це підтверджує універсальність мультимедійних технологій не лише в розвагах, а й у науці, освіті та виробництві.

Мультимедійні технології також розвиваються у сфері мережевої взаємодії. Хмарні ігрові сервіси, як-от *NVIDIA GeForce NOW* чи *Xbox Cloud Gaming*, вимагають передачі високоякісних мультимедійних потоків із мінімальною затримкою. Для цього використовуються алгоритми стиснення відео (*AV1*, *H.265*), мережеві протоколи адаптивної трансляції (*WebRTC*, *RTP*) та буферизація аудіо-візуальних даних. Таким чином, мультимедійні технології стають основним технічним ядром, від якого залежить стабільність і якість користувацького досвіду у потокових ігрових сервісах.

Висновок

Використання мультимедійних технологій у розробці ігрових застосунків забезпечує поєднання візуальних, звукових та інтерактивних компонентів у єдину функціональну систему. Інтеграція процедурної генерації, XR-технологій та штучного інтелекту підвищує реалістичність, адаптивність і ефективність процесу розробки. Мультимедіа виступає ключовим фактором формування користувацького досвіду та визначає подальший розвиток геймдизайну.

Список використаних джерел

1. Hendrikx M., Meijer S., van der Velden J., Iosup A. (2011). *Procedural Content Generation for Games.* ACM Trans. Multimedia Comput. Commun. Appl. URL: https://madoc.bib.uni-mannheim.de/59000
2. Togelius J., Snodgrass S., Guzdial M. et al. (2017). *Procedural Content Generation via Machine Learning.* arXiv:1702.00539. URL: https://arxiv.org/abs/1702.00539
3. PURL (NSF). (2023). Deep Learning for Procedural Content Generation: A Survey. URL: https://arxiv.org/abs/2305.00644
4. Gunkel S.N.B., Potetsianakis E., Klunder T.E., Toet A., Dijkstra-Soudarissanane S. (2022). *Immersive Experiences and XR: A Game Engine or Multimedia Streaming Problem?* arXiv:2201.05552. URL: https://arxiv.org/abs/2201.05552
5. Wang H., Dong J. et al. (2023). Immersive Multimedia Communication: State-of-the-Art on XR Streaming. ACM Digital Library. URL: https://dl.acm.org/doi/10.1145/3721292
6. ResearchGate (2023). *Procedural Content Generation: An Overview.* URL: https://www.researchgate.net/publication/345882435_Procedural_Content_Generation_An_Overview

7. Springer (2012). *Serious Games and Their Applications in Education.* URL: https://link.springer.com/chapter/10.1007/978-3-642-27355-1_3
8. *Journal of Multimedia Technology and Trends (2023).* URL: https://journal.educol-labs.org/index.php/JMTT/issue/archive

Ключові слова: генеративний ШІ.
Keywords: generative AI.

АНАЛІЗ СУЧАСНОГО СТАНУ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Світличний Дмитро

Національний технічний університет «Харківський політехнічний інститут», аспірант кафедри кібербезпеки

У сучасному світі розвиток технологій призвів одночасно до вдосконалення та прогресу атак і загроз у сфері кібербезпеки на об'єкти критичної інфраструктури (ОКІ). Такі атаки відбуваються кожний день, або, якщо брати до уваги ОКІ по всій планеті, постійно. Це зумовлює високий пріоритет для створення захисту та протидії цим атакам. Першочерговим завданням є дослідження, аналіз та класифікація атак на ОКІ.

Сучасні дослідження [1-3] показують, що цифровізація, конвергенція управління інформацією та даними (Information Technology, IT) із управлінням і контролем фізичних процесів і устаткуванням (Operational Technology, OT) та масове підключення пристроїв збільшують площу атаки й створюють умови для складних кібератак на ОКІ з наслідками для нацбезпеки та економіки.

Найпоширеніші загрози для ОКІ [1]:

- шкідливе програмне забезпечення,
- програми-вимагачі,
- фішинг,
- розподілена атака типу "Відмова в обслуговуванні" (DDoS),
- атака нульового дня (zero-day),
- атаки на ланцюг постачання,
- довготривалі розширені постійні загрози.

Для енергетики ризики підсилюють легасі-системи, інтеграція IT та OT і швидке зростання Інтернету речей (Internet of Things, IoT) (сенсори, смарт-

лічильники, тощо), що розширює вектори атак і ускладнює захист операційних технологій. Згідно до роботи [1], підкреслюється основні три групи проблем:

- технічні (легасі системи контролю та збору даних, легасі системи промислового контролю, інтеграція IT та OT, IoT),
- організаційні (низька обізнаність, дефіцит кадрів, відсутність політик),
- регуляторні (строгі, але не завжди практичні вимоги).

Рішення: застосування штучного інтелекту (ШІ) та машинного навчання (МН) для виявлення аномалій у мережевому трафіку, блокчейну для захисту транзакцій і даних смарт-мереж, регулярних аудитів, інцидент-планів і тренінгів для персоналу. Важлива роль публічно-приватних партнерств для обміну даними.

Для виявлення атак на ОКІ існують різні технології на базі ШІ та МН. У роботі [4] було продемонстровано використання моделі МН Початок (Inception) для аналізу датасету UNSW-NB15. Результати: точність (частка правильно класифікованих прикладів, як атак, так і нормального трафіку) 98.40%, влучність (відсоток коректно визначених атак серед усіх, які модель позначила як загрози) 99%, впізнавання (здатність моделі виявляти реальні атаки серед усіх наявних атак) 97.9%, оцінка F1 (узагальнений показник, що поєднує влучність і впізнавання та свідчить про збалансовану роботу моделі) 98.5%. Порівняння з іншими моделями МН Випадковий ліс (Random Forest), k найближчих сусідів (k-Nearest Neighbors) та багатошаровий перцептрон (Multi-Layer Perceptron) довело перевагу глибокого навчання у масштабованості та точності. Практичні можливості для застосування на ОКІ:

- інтеграція сигнатурного, поведінкового та аномального аналізу;
- пояснюваний ШІ;
- застосування технології Оркестрації безпеки, автоматизації та реагування.

Для систематизації безпеки ОКІ використовуються рамки та стандарти (фреймворки). У роботі [2] через систематичний огляд спеціалізованої літератури було показано, що NIST фреймворк для кібербезпеки (Cybersecurity Framework, CSF), ISO/IEC 27001 та CIS Controls є найпоширенішими фреймворками. Вони задають основу для створення кібербезпеки ОКІ, але мають недоліки:

- нестача секторної адаптивності (енергетика, охорона здоров’я та інші),

- слабка інтеграція ШІ, МН та блокчейну,
- ігнорування людського фактора (помилки, необізнаність, соціальна інженерія та інші).

Пропонований новий фреймворк містить п'ять компонентів [2]:

- оцінка ризиків,
- інцидент-менеджмент,
- контроль доступу,
- розвиток стійкості,
- управління.

Валідовані кейси у сфері охорони здоров'я показали: скорочення часу реагування на 75%, зменшення несанкціонованого доступу на 40%, покращення стійкості на 60%.

Управління, процеси та людський фактор також розглядаються у роботі [3]. Було показано, що 12 із найчастіше описаних інцидентів у ОКІ пов'язані з людськими помилками:

- слабкі паролі,
- відсутність тренінгів,
- низька обізнаність керівництва.

В межах дослідження [3] для покращення протидії кіберзагрозам було зроблено мапування кіберзагроз на функції NIST CSF. Особливо було підкреслено наступні функції: ID.GV (управління), PR.AT (навчання), DE.CM (моніторинг), RS.RP (планування реагування) та RC.RP (план відновлення).

У підсумку, беручи до уваги наведені вище види кіберзагроз, вектори потенційних атак, засоби захисту, попередження та протидії небезпеці, управління та відновлення ОКІ, отримуємо наступні практичні рекомендації згідно до [1-4]:

1. Повна інвентаризація IT та OT активів та класифікація даних.
2. Сегментація мереж OT, нульовий рівень довіри доступу (Zero Trust), контроль доступу постачальників.
3. Використання ШІ та МН для виявлення аномалій у трафіку та предикативної аналітики.
4. Застосування блокчейну для безпечних транзакцій у енергомережах.
5. Регулярні аудити та навчання з ліквідації наслідків стихійних лих.
6. Тренінги співробітників та симуляції фішингових атак.

7. Перехід до кванто стійкої криптографії.
8. Забезпечення відповідності NIST, ISO/IEC 27001, IEC 62443, NERC-CIP.

Дослідження показало, що ефективний захист ОКІ можливий лише через комплексний підхід: фреймворки управління ризиками (NIST CSF та розширені моделі), використання ШІ, МН та блокчейну, посилення людського фактору через навчання, а також співпраця держави та приватних структур. Особливий акцент має бути на енергетиці, де поєднання легасі-систем та нових технологій створює критичні ризики.

Список використаної літератури:

1. Ajayi O., Alozie C., Abieba O. Enhancing Cybersecurity in Energy Infrastructure: Strategies for Safeguarding Critical Systems in the Digital Age. Trends in Renewable Energy. 2025. Vol. 11, No. 2. P. 201-212.
2. Alozie C., Chinwe E. Developing a Cybersecurity Framework for Protecting Critical Infrastructure in Organizations. Iconic Research And Engineering Journals. 2025. Vol. 8, No. 7. P. 562-576.
3. Shah S. Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure. Journal of Global Research in Electronics and Communication. 2025. Vol. 2, No. 2. P. 1-6.
4. Aljumaiah O., Jiang W., Addula S., Almaiah M. Analyzing Cybersecurity Risks and Threats in IT Infrastructure based on NIST Framework. Journal of Cyber Security and Risk Auditing. 2025. Vol. 2025, No. 2. P. 12-26.

Ключові слова: кібербезпека, об'єкти критичної інфраструктури (ОКІ), штучний інтелект (ШІ), NIST фреймворк для кібербезпеки.
Keywords: cybersecurity, critical infrastructure facilities (CIF), artificial intelligence (AI), NIST Cybersecurity Framework (NIST CSF).

АНАЛІЗ ІНСТРУМЕНТІВ ТА ПЛАТФОРМ ДЛЯ ТРЕКІНГУ ЕКСПЕРИМЕНТІВ

Савенко Михайло

Національний університет «Одеська юридична академія»,
студент факультету кібербезпеки та інформаційних технологій

У сучасному науковому середовищі, де машинне навчання стає ключовим елементом інноваційних розробок, трекінг експериментів набуває критичного значення як засіб забезпечення відтворюваності, порівнянності та ефективності дослідницьких процесів. Трекінг експериментів охоплює систематичний збір, зберігання та аналіз метаданих, параметрів, метрик продуктивності та артефактів, що виникають під час ітеративних циклів

розробки моделей, від підготовки даних до розгортання в продуктивне середовище. Цей процес не лише полегшує виявлення оптимальних конфігурацій моделей, але й сприяє колективній роботі команд, дозволяючи уникнути дублювання зусиль і полегшуючи аудит результатів.

Одним з фундаментальних аспектів трекінгу є забезпечення відтворюваності, яка досягається через фіксацію всіх вхідних та вихідних параметрів експерименту. Уявіть типовий цикл: дослідник вибирає датасет, налаштовує гіперпараметри мережі, запускає тренування на графічному процесорі та оцінює модель за допомогою кросвалідації. Без трекінгу цей процес перетворюється на ланцюг непередбачуваних подій, де успішний результат важко повторити через зміни у версіях бібліотек чи то випадкові фактори. Сучасні платформи вирішують цю проблему, впроваджуючи автоматизовані хуки для логування, які активуються на етапі ініціалізації тренування. Такі системи не лише зберігають числові метрики, як-от точність чи функцію втрат, а й фіксують текстові описи, знімки градієнтів та навіть логи обчислень, дозволяючи провести ретроспективний аналіз.

Інтеграція трекінгу з пайплайнами автоматизації, такими як оркестрація робочих потоків, підвищує ефективність на 30-50%, оскільки дозволяє автоматизувати гіперпараметричний пошук і моніторинг дрейфу даних. Це особливо актуально для великих команд, де колаборація вимагає централізованого доступу до історії експериментів, з можливістю коментування та розподілу ролей [1].

З-посеред інших платформа **MLflow** вирізняється своєю універсальністю як відкрита система для керування життєвим циклом машинного навчання. Вона складається з кількох компонентів, де модуль трекінгу дозволяє фіксувати параметри, метрики та артефакти для кожного запуску, створюючи ієрархію проєктів і експериментів. Користувач може запустити сервер трекінгу локально або в хмарі, після чого через програмний інтерфейс логуються дані в реальному часі з можливістю фільтрації за тегами чи значеннями метрик. Перевагою MLflow є інтеграція з різними мовами програмування та фреймворками, що робить її ідеальною для гетерогенних середовищ, де команди використовують як Python, так і R [2]. На практиці це дозволяє провести серію експериментів з варіаціями архітектури, автоматично генеруючи звіти про продуктивність, без потреби ручного копіювання файлів. Дослідження артефактів життєвого циклу підкреслює, що MLflow досягає високого рівня покриття критеріїв логування та версіонування, перевершуючи базові інструменти за інтеграцією з оркестраторами, як-от Kubeflow. Однак, для великих обсягів даних, де потрібна розподілена обробка, MLflow рекомендується комбінувати з інструментами версіонування, щоб уникнути перевантаження локального сховища [3].

Іншою потужною платформою є **Weights & Biases**, яка орієнтована на візуалізацію та колаборацію в процесі трекінгу. Ця система автоматично відстежує метрики під час тренування, генеруючи інтерактивні панелі з графіками втрат, матрицями плутанини та гістограмами гіперпараметрів, що полегшує інтерпретацію складних траєкторій. Користувачі можуть створювати «свіпи» – масові запуски з варіаціями параметрів, – і миттєво порівнювати результати через паралельні криві, виявляючи оптимальні точки. У контексті командної роботи Weights & Biases надає робочі простори для спільного редагування з нотифікаціями про завершення експериментів та інтеграцією з системами контролю версій [4]. Ця платформа вирізняється обробкою програмних артефактів, дозволяючи фіксувати залежності та середовища, що критично для відтворюваності в мультиплатформових проєктах. Попри хмарну орієнтацію, яка забезпечує масштабованість, користувачі відзначають потребу в локальних опціях для чутливих даних, де конфіденційність переважає зручність [5].

Платформа **Neptune.ai** акцентована на метаданих як на основі трекінгу. Вона пропонує централізоване сховище для датасетів, моделей і логів експериментів. Через програмний інтерфейс дослідник може маркувати запуски тегами, додавати кастомні метрики та прикріплювати артефакти, як-от: знімки моделей чи то звіти. Візуальний дашборд дозволяє будувати кастомні запити, фільтрувати експерименти за продуктивністю або часом виконання, з можливістю експорту в формати для подальшого аналізу. Neptune.ai здатна значно знизити помилки в постекспериментальних задачах, досягаючи 7% рівня помилок проти 48% без інструментів, завдяки інтуїтивному інтерфейсу для порівнянь [3]. Ця платформа корисна для академічних середовищ, де потрібно документувати процеси для публікацій, але вимагає навчання для повного використання автоматизованих пайплайнів.

Інструмент **Sacred** пропонує мінімалістичний підхід до конфігурації та логування, інтегруючись безпосередньо в скрипти тренування. Він фіксує конфігурації як YAML-файли, автоматично генерує ідентифікатори для запусків і дозволяє моніторити метрики через бази даних чи файли [6]. Sacred вирізняється можливістю редагування конфігурацій без перезапуску коду, що прискорює ітерації, та інтеграцією із системами моніторингу для реального часу. Недоліком є обмежена візуалізація, що робить його доповненням до графічних платформ [1].

Платформа **ClearML**, як частина екосистеми MLOps, автоматизує трекінг через «магічні» хуки, що активуються без значних змін у коді, фіксуючи все від ресурсів до артефактів [2]. Вона підтримує віддалене виконання на кластерах, з дашбордом для моніторингу кількох запусків паралельно. ClearML здатна на високу автоматизацію колекції, аж до 64% непрямої

фіксації, що зменшує навантаження на розробників [1]. У промислових проєктах це дозволяє масштабувати експерименти на тисячі ядер, але вимагає налаштування сервера для приватних розгортань.

Інструмент **DVC** (Data Version Control) розширює традиційний контроль версій на дані та моделі через трекінг метафайлів, які посилаються на хеші файлів. Він інтегрується з Git для повного відтворення пайплайнів, дозволяє кешувати проміжні результати та порівнювати версії датасетів [7]. Це робить його ідеальним для відкритих проєктів, де прозорість коду є пріоритетом.

Платформа **Comet.ml** фокусується на оптимізації, пропонуючи інструменти для автоматизованого трекінгу гіперпараметрів та A/B-тестування моделей. Вона генерує звіти з тепловими картами продуктивності і дозволяє виявляти кореляції між параметрами. Її сильними сторонами є обробка залежностей та інтеграція з моніторингом для постпродакшну. Користувачі цінують мобільність інтерфейсу, але критикують вартість для великих команд [5].

Для прозорості трекінгу розроблено інструмент **PyPads**, який забезпечує неінтрузивне логування без змін у коді, фіксує контекст виконання через декоратори. Він створює структуровані логи з метаданими, доступними для аналізу в Jupyter [8]. PyPads корисний в освітніх проєктах, де студенти потребують детального трасування.

Метамодель **EMMM** пропонує уніфікований фреймворк для трекінгу, який стандартизує метадані через абстрактну модель, що інтегрується з наявними платформами. Вона визначає сутності як експерименти, активи та залежності, дозволяє кросплатформову міграцію. Важливою є її роль у зменшенні фрагментації і забезпеченні семантичної узгодженості. У майбутніх розробках це може стати основою для API-стандартів [9].

Подальший розвиток трекінгу стосується інтеграції з AutoML, де інструменти автоматично генерують експерименти, фіксуючи еволюцію пошуку. У проєктах з великими мовними моделями трекінг розширюється на моніторинг токенів та етичних метрик, запобігаючи упередженням.

Наявні інструменти формують екосистему, де трекінг не є ізольованою функцією, а частиною інтегрованого ланцюга, що підвищує наукову цінність досліджень. Їх вибір залежить від масштабу проєкту з акцентом на відкриті рішення для академії та хмарні для індустрії.

Список використаних джерел:

1. Hewage D., Meedeniya D. Machine Learning Operations: A Survey on MLOps Tool Support. *Arxiv.* 2022. Vol. 2202. P. 1-12. DOI: https://doi.org/10.48550/arXiv.2202.10169
2. Ruggeri D., Tazza G., Vidács L. Introducing MLOps to Facilitate the Development of Machine Learning Models in Agronomy: A Case Study. *IEEE Access.* 2025. DOI: https://doi.org/10.1109/ACCESS.2025.3586691

3. Berberi L., Kozlov V., Alibabaei Kh., Sanchis B. MLflow and its usage. *AI4EOSC Platform: Users' Workshop.* 2023. DOI: https://doi.org/10.13140/RG.2.2.32801.17761.
4. W&B Models. URL: https://docs.wandb.ai/models.
5. Idowu S., Strüber D., Berger T. Asset management in machine learning: A survey. IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP). 2021. P. 51-60. DOI: https://doi.org/10.1109/ICSE-SEIP52600.2021.00014
6. Idowu S., Osman O., Strüber D. et al. Machine learning experiment management tools: a mixed-methods empirical study. *Empir Software Eng*. 2024. Vol. 29, 74. DOI: https://doi.org/10.1007/s10664-024-10444-w
7. Barrak A., Eghan E. E., Adams B. On the co-evolution of ml pipelines and source code-empirical study of dvc projects. *IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER).* 2021. March. P. 422-433. IEEE. DOI: https://doi.org/10.1109/SANER50967.2021.00046.
8. Weißgerber T., Amor M. B., Fellicious C. et al. PyPads. *Datenbank Spektrum*. 2024. Vol. 24. P. 53-62. DOI: https://doi.org/10.1007/s13222-023-00459-w.
9. Idowu S., Strüber D., Berger T. EMMM: A Unified Meta-Model for Tracking Machine Learning Experiments. *48th Euromicro Conference on Software Engineering and Advanced Applications (SEAA).* 2022. P. 48-55. DOI: https://doi.org/10.1109/SEAA56994.2022.00016.

Ключові слова: вебдизайн, вебпрограмування, візуалізація, колір.
Keywords: web design, web programming, visualization, color.

Науковий керівник: к.т.н., доцент Трофименко О.Г.

АРХІТЕКТУРНІ ТА АЛГОРИТМІЧНІ ВИКЛИКИ НАВЧАННЯ ASR-МОДЕЛЕЙ ДЛЯ РОЗПІЗНАВАННЯ УКРАЇНСЬКОГО МОВЛЕННЯ

Антіпіна Надія

Національний університет «Одеська юридична академія»,
студентка факультету кібербезпеки та інформаційних технологій

На відміну від класичних задач класифікації, розпізнавання мовлення має свої характерні особливості. У системах розпізнавання мовлення (ASR-системах) модель має навчитися перетворювати довгу послідовність звукових фреймів у значно коротшу послідовність символів без чіткої відповідності довжин між вхідними та вихідними послідовностями. Щоб вирішити цю проблему, додається алгоритм CTC (Connectionist Temporal Classification), який допомагає моделі самостійно навчитися вирівнювати аудіопослідовності змінної довжини з відповідними текстовими транскрипціями змінної довжини без необхідності зазначення точних часових проміжків кожного символу [1]. Також під час роботи з великими нейронними мережами виникає ризик перенавчання, коли через недостатню кількість прикладів система

запам’ятовує приклади з навчальної вибірки, але не узагальнює закономірність та через це має низький показник точності на тестових даних. Щоб уникнути цього явища, у ASR-системах потрібно застосовувати методи регуляризації (наприклад, Dropout, Weight Decay та Batch Normalization).

Процес навчання моделі розпізнавання мовлення стосується використання великих обсягів даних з тисячів годин аудіозаписів з точними транскрипціями, а якість та репрезентативність цих даних безпосередньо визначають якість майбутньої моделі. Для досягнення високої точності розпізнавання важливо, щоб навчальні дані охоплювали різні варіанти вимови, інтонації, темпу, діалектів, вікових особливостей мовців і умов навколишнього середовища. Тим самим модель отримує здатність ефективно узагальнювати закономірності та розпізнавати різні варіанти людського мовлення. Рівень складності мови, специфічність предметної області, вимоги до різноманітності прикладів в зв'язку з ризиком перенавчання суттєво збільшують складність підбору навчальних даних [2]. Оскільки аудіосигнал є неперервним за часом і характеризується значними варіаціями гучності, частоти та спектрального складу, перед подачею в нейронну мережу проводиться підготовка вхідних даних, де сигнал проходить попередню обробку в декілька стадій, лише після чого параметри стають вхідними ознаками для моделі. Також ASR-модель повинна навчатися працювати з часовими залежностями між сусідніми звуками або словами, отже під час навчання використовуються великі вікна часових фреймів, які дозволяють мережі сприймати мовлення як послідовний сигнал, а не як набір ізольованих звуків, а також залучаються рекурентні чи двонаправлені мережі для врахування контексту. Через це навчання ASR-моделей вимагає великих обсягів пам’яті та часу, а також складної архітектури реалізації.

В контексті розпізнавання української мови навчання моделі ускладнюється обмеженістю мовних ресурсів, адже датасети, що містять записи з низькою якістю або нерівномірним представленням різних діалектів, темпів мовлення та соціальних груп несуть ризик перенавчання моделі на дикторське мовлення та втрати точності розпізнавання мови в реальних умовах. Дослідження [3] відносить українську мову до числа малоресурсних мов. Недостатня узгодженість серед датасетів стандартів транскрипції для міток може призвести до неоднозначності між звуковим і текстовим представленням та відсутності стабільності, що впливає на якість процесу навчання моделі. Різноманітність діалектів та суттєва різниця в мовленні, акцентах, словниках представників різних областей України теж є складною задачею для узагальнення навіть сучасними нейронними мережами. Крім того, українська мова має обмежену підтримку в популярних фреймворках, що використовуються для розробки мереж глибинного навчання (TensorFlow, PyTorch та інші), більшість сучасних архітектур систем розпізнавання

мовлення оптимізовані для англійської мови та потребують адаптування або навчання для розпізнавання української. Також для англійської мови є великі тестові набори (LibriSpeech, CommonVoice), створені для об'єктивної оцінки та вимірювання точності результатів моделей, аналогів чого для української мови бракує.

Отже навчання у системах автоматичного розпізнавання мовлення має низку характерних особливостей: воно вимагає великих наборів мічених даних, спеціальних алгоритмів для узгодження послідовностей та врахування контексту, складної попередньої обробки сигналів і потужних обчислювальних ресурсів. Побудова моделі розпізнавання українського мовлення ускладнюється меншою кількістю ресурсів – навчальних датасетів та технічних засобів, адаптованих для роботи з українською мовою.

Список використаної літератури:

1. Automatic Speech Recognition using CTC. URL: https://www.geeksforgeeks.org/nlp/automatic-speech-recognition-using-ctc
2. Wang C., Wu Y., Liu S., Li J., Qian Y., Kumatani K., Wei F. UniSpeech at scale: An Empirical Study of Pre-training Method on Large-Scale Speech Recognition Dataset. arXiv. 2021. DOI: https://doi.org/10.48550/arXiv.2107.05233
3. Silovsky J., Deng L., Argueta A., Arvizo T., Hsiao R., Kuznietsov S., Lin Y., Xiao X., Zhang Y. Cross-lingual Knowledge Transfer and Iterative Pseudo-labeling for Low-Resource Speech Recognition with Transducers. arXiv. 2023. DOI: https://doi.org/10.48550/arXiv.2305.13652

Ключові слова: рушій, розробка ігор, графіка, Unity, Godot, Unreal Engine.
Keywords: engine, gamedev, graphics, Unity, Godot, Unreal Engine.

Науковий керівник: к.т.н., доцент Трофименко О.Г.

АРХІТЕКТУРА ТА ОСНОВНІ КОМПОНЕНТИ AUTOML-СИСТЕМ

Лобода Юлія

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат педагогічних наук, доцент

Дерев'ягін Владислав

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Автоматизоване машинне навчання (AutoML) один із ключових напрямів розвитку сучасної аналітики даних, оскільки забезпечує можливість створення моделей машинного навчання без необхідності глибокої експертної участі. Класичний процес розроблення моделей включає низку послідовних етапів від збору та препроцесингу даних до вибору моделі та оптимізації її

гіперпараметрів, які потребують значних часових і інтелектуальних ресурсів [1].

AutoML-системи дозволяють навчати високоякісні моделі автоматично, використовуючи комплекс алгоритмів для формування пайплайнів, пошуку моделей та оптимізації параметрів. В умовах зростання обсягів даних, збільшення складності моделей та потреби у швидкому отриманні результатів AutoML стає важливим інструментом як для наукових досліджень, так і для промислових застосувань.

Метою дослідження є аналіз архітектурних принципів сучасних AutoML-систем, структурних компонентів ML-пайплайна та методів оптимізації гіперпараметрів, які визначають продуктивність і якість автоматизованого моделювання.

AutoML-системи ґрунтуються на модульній архітектурі, у якій кожен компонент відповідає за певний етап підготовки та побудови моделі.

Структура AutoML включає такі ключові елементи:

– модуль препроцесингу даних, що виконує автоматичну обробку пропусків, аномалій, масштабування числових ознак та кодування категорій;

– модуль інженерії та відбору ознак, який підтримує автоматичну генерацію ознак та інтелектуальний відбір найбільш інформативних характеристик;

– модуль вибору моделі, що тестує широкий спектр алгоритмів від лінійних моделей до ансамблевих методів і нейронних мереж;

– модуль оптимізації гіперпараметрів як центральний компонент архітектури;

– модуль ансамблювання моделей для підвищення стабільності та точності;

– модуль оцінювання та вибору найкращої моделі [2].

Для системного описання AutoML-систем використовують формальні поняття: оператор пайплайна як окрема операція над даними; пайплайн як впорядкована послідовність операторів; простір пошуку як множина усіх можливих пайплайнів; оптимізаційна задача як вибір оптимального пайплайна, що мінімізує функцію втрат на валідаційних даних. Розмір простору пошуку може сягати мільйонів варіантів навіть для простих задач, що робить вибір ефективного методу оптимізації критично важливим.

Класичні методи оптимізації включають Grid Search – повний перебір дискретних конфігурацій з експоненційною складністю, та Random Search – випадкове дослідження простору параметрів, яке часто виявляється ефективнішим у високорозмірних просторах [3]. Просунуті методи представлені байєсовою оптимізацією, яка будує модель функції втрат; bandit-методами, що забезпечують оптимальний розподіл обчислювальних ресурсів через Successive Halving, Hyperband та BOHB; еволюційними алгоритмами,

ефективними в складних і нерегулярних просторах [4,5]. Спеціалізовані підходи включають Neural Architecture Search для автоматичного пошуку архітектур нейронних мереж та Meta-Learning для використання історичних знань (warm-start, transfer learning та learning curves prediction).

Проведений аналіз методів показує, що Grid Search забезпечує гарантоване знаходження оптимуму в обраному просторі, але має низьку швидкість збіжності та погану масштабованість. Random Search демонструє кращу масштабованість при середній швидкості збіжності. Байєсова оптимізація досягає високої швидкості збіжності та відмінної якості рішень, але має середню масштабованість та високу складність реалізації. Hyperband та BOHB поєднують дуже високу швидкість збіжності з відмінною масштабованістю, що робить їх найперспективнішими для сучасних AutoML-систем.

Практичні реалізації AutoML-систем включають Auto-sklearn, який використовує SMAC і мета-навчання для warm-start; H2O AutoML – платформу з підтримкою розподіленого навчання; TPOT, що використовує генетичне програмування; а також хмарні рішення Google Cloud AutoML та Azure AutoML, які застосовують NAS для побудови глибоких моделей [6].

В результате аналізу архітектури AutoML-систем та їх оптимізаційних механізмів встановлено, що ефективність AutoML визначається узгодженою взаємодією модулів препроцесингу, інженерії ознак, вибору моделей, оптимізації гіперпараметрів та оцінювання. AutoML-системи поєднують різні оптимізаційні техніки, забезпечуючи баланс між точністю, швидкістю та обчислювальною ефективністю. Найперспективнішими є гібридні методи, що комбінують переваги різних підходів, зокрема BOHB як комбінація байєсової оптимізації та Hyperband. Огляд сучасних платформ підтверджує ефективність модульного проєктування AutoML-систем і демонструє різноманітність підходів до реалізації архітектури. Отримані результати можуть бути використані як теоретична основа для подальших досліджень AutoML-пайплайнів, створення експериментальних оптимізаційних систем та побудови автоматизованих рішень у задачах Data Science.

Список використаної літератури:

1. Del Valle A.M., Mantovani R.G. & Cerri R. A systematic literature review on AutoML for multi-target learning tasks. *Artif Intell Rev.* 2023. 56 (Suppl 2), pp. 2013–2052. https://doi.org/10.1007/s10462-023-10569-2.
2. Karl F., Thomas J., Elstner J., Gross R., Bischl B. Automated Machine Learning. *Unlocking Artificial Intelligence*. Springer, Cham. 2024, pp. 3–25. https://doi.org/10.1007/978-3-031-64832-8_1.
3. Liashchynskyi P., Liashchynskyi P. Grid search, random search, genetic algorithm: a big comparison for NAS. *arXiv preprint*. 2019. https://doi.org/10.48550/arXiv.1912.06059.

4. Dôres S.C.N., Soares C. Bandit-Based Automated Machine Learning. *2018 7th Brazilian Conference on Intelligent Systems (BRACIS)*, Sao Paulo, Brazil, 2018, pp. 121-126, DOI: 10.1109/BRACIS.2018.00029
5. Falkner S. et al. BOHB: Robust and efficient hyperparameter optimization at scale. *International conference on machine learning*. PMLR, 2018. P. 1437–1446. https://doi.org/10.48550/arXiv.1807.01774
6. SMAC: Sequential Model-based Algorithm Configuration. URL: https://www.cs.ubc.ca/labs/algorithms/Projects/SMAC/

Ключові слова: автоматизоване машинне навчання, машинне навчання, гіперпараметри, оптимізація, архітектура систем, пайплайн.
Keywords: AutoML, machine learning, hyperparameters, optimization, system architecture, pipeline.

ІНТЕЛЕКТУАЛЬНИЙ ЧАТ-БОТ ДЛЯ НАВЧАННЯ АНГЛІЙСЬКОЇ МОВИ: АРХІТЕКТУРА ТА ФУНКЦІОНАЛЬНА МОДЕЛЬ

Трофименко Олена
доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Безродний Микола
студент факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»,

Процес навчання англійської мови в цифровому середовищі зазнав суттєвих трансформацій під впливом технологій дистанційної комунікації, мобільних платформ та інтелектуальних освітніх агентів. Автоматизація навчання іноземних мов є одним із ключових напрямів цифрової трансформації освітнього процесу, що поєднує методологію лінгводидактики з інструментами штучного інтелекту (ШІ), обробки природної мови (NLP) та адаптивного навчання. Завдяки інтеграції з базами знань, NLP-модулями та аналітичними інструментами, такі системи здатні не лише фіксувати прогрес користувача, а й формувати персоналізовані траєкторії навчання [1]. Особливої актуальності набуває використання чат-ботів як інтерфейсів освітньої взаємодії, що поєднують діалогову форму навчання з когнітивною підтримкою [2].

Запропонована архітектура інтелектуального чат-бота для навчання англійської мови (рис. 1) реалізує трирівневу модель взаємодії, що забезпечує модульність, масштабованість та персоналізацію навчального процесу відповідно до індивідуальних потреб користувача. Система складається з трьох функціональних рівнів: Frontend (інтерфейсний рівень), Backend (серверний рівень обробки) та Data Layer (рівень зберігання даних). Такий

підхід відповідає сучасним принципам проєктування розподілених інформаційних систем, де кожен рівень виконує чітко визначені функції та взаємодіє з іншими через стандартизовані API-інтерфейси.

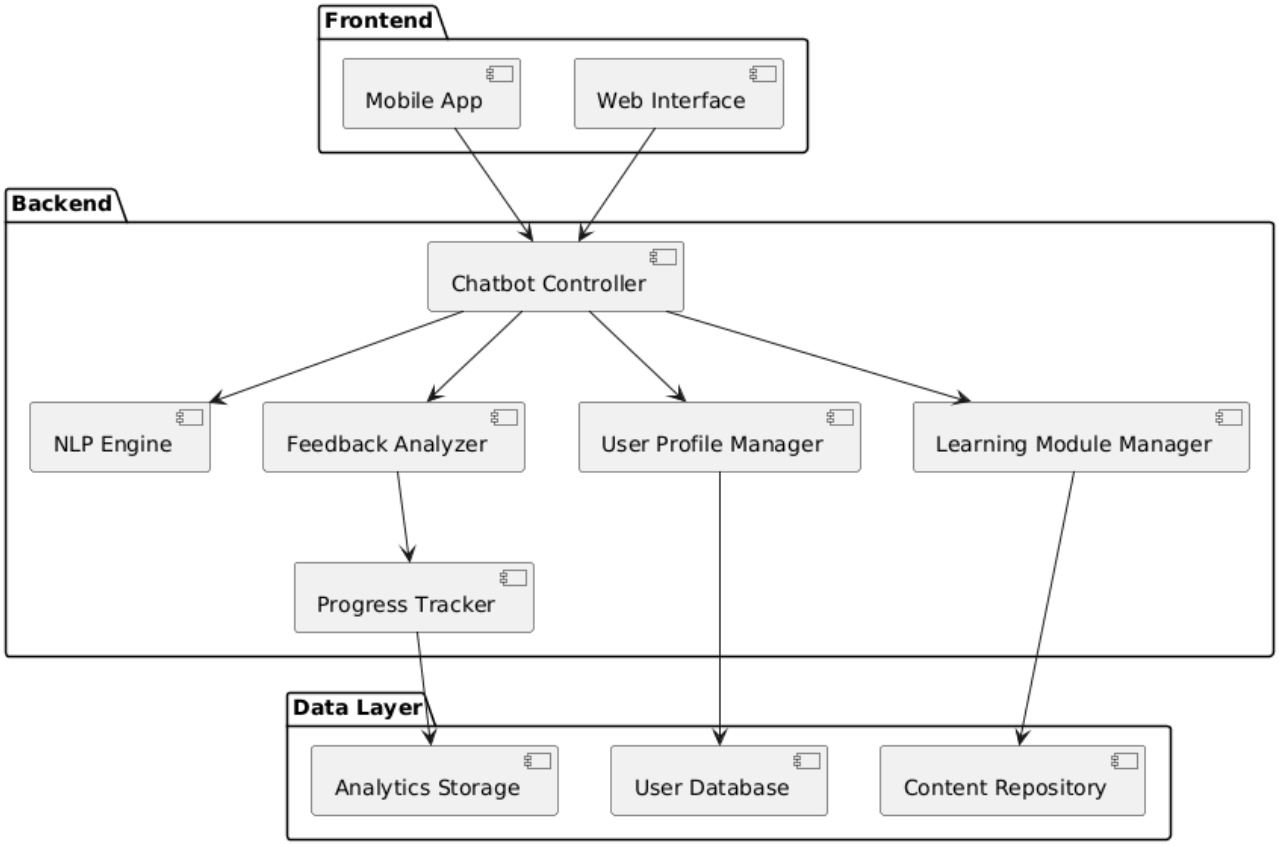

Рисунок 1 – Трирівнева архітектура освітнього чат-бота: інтерфейс, логіка обробки та зберігання дани

Ключовою особливістю запропонованої архітектури є центральна роль Chatbot Controller як оркестратора всіх взаємодій між компонентами системи. Цей компонент забезпечує координацію роботи NLP-модулів, аналітичних інструментів та системи персоналізації, формуючи когерентний освітній досвід для користувача. На відміну від традиційних систем електронного навчання, де взаємодія обмежується статичним контентом, запропонована архітектура реалізує динамічний діалоговий підхід з адаптивним управлінням складністю навчального матеріалу.

На інтерфейсному рівні Mobil App (мобільний застосунок) та Web Interface (вебінтерфейс) реалізують принцип повсюдного навчання – можливості здобувати знання в будь-який час і в будь-якому місці. Дослідження показують, що мобільні платформи для вивчення мов підвищують залученість студентів на 34–42% завдяки сповіщенням, мікронавчанню та елементам ігровізації [3]. Обидва інтерфейси мають діалоговий інтерфейс з підтримкою текстового та голосового введення, систему відстеження прогресу з візуалізацією показників (щоденні серії, завершені уроки, засвоєні слова) та інтеграцію технологій розпізнавання та синтезу мовлення для практики

вимови. Вебверсія додатково надає розширену аналітику з графіками навчального прогресу, можливістю експорту матеріалів у PDF та підтримкою групових вправ для взаємодії між користувачами.

З технічного боку Frontend взаємодіє з Backend через прикладні програмні інтерфейси (RESTful API) для базових (CRUD) операцій з даними та через двосторонній канал обміну повідомленнями (WebSocket) з мінімальною затримкою (до 100 мс). Технологія маркування доступу (JWT-токенізація) забезпечує безпечну та безперебійну роботу на різних пристроях

На серверному рівні взаємодіють контролер чат-бота (Chatbot Controller), модуль обробки природної мови (NLP Engine), аналізатор відповідей (Feedback Analyzer), менеджер профілю користувача (User Profile Manager), модуль навчального контенту (Learning Module Manager) та трекер прогресу (Progress Tracker).

Chatbot Controller виконує роль центрального координатора, який керує обробкою запитів, підтримує контекст діалогу, агрегує відповіді та забезпечує стійкість взаємодії на основі патерна Mediator. Реалізація базується на асинхронній подієвій архітектурі, що дозволяє обробляти сотні одночасних звернень.

NLP Engine розпізнає наміри користувача та аналізує мовну правильність. Використовується донавчена модель BERT для класифікації запитів (grammar_question, vocabulary_request, exercise_answer, free_conversation), а також інструменти синтаксичного аналізу та виявлення граматичних помилок (subject-verb agreement, article usage, tense consistency) з генерацією пояснень та прикладів коректного використання. Аналізатор відповідей оцінює правильність, лексичне різноманіття, типові помилки та емоційний стан користувача, передаючи результати до трекера прогресу.

Feedback Analyzer оцінює відповіді користувача за кількома критеріями: correctness assessment через rule-based порівняння або semantic similarity аналіз (BERT embeddings), lexical diversity analysis (Type-Token Ratio, MTLD метрики), error pattern detection через machine learning моделі та sentiment analysis для виявлення frustration. Результати передаються до Progress Tracker для формування learning analytics.

User Profile Manager реалізує концепцію Learner Model – структуру знань, навичок, помилок і вподобань, яка використовується для адаптації навчального контенту. Модуль навчання формує індивідуальні траєкторії на основі педагогічних принципів та рівня володіння мовою, використовуючи теорію відповідності завдань, систему повторення з інтервалами та чергування типів вправ. Трекер прогресу накопичує дані про навчальну активність, прогнозує ризики втрати знань і рекомендує наступні кроки.

Learning Module Manager формує персоналізовані навчальні траєкторії на основі Learner Model та педагогічних принципів. Контент структуровано

відповідно до CEFR дескрипторів з prerequisite topics для кожного рівня. Інтегровано Leitner system для spaced repetition лексики та принцип interleaving різних типів вправ, що підвищує long-term retention на 30-40% [3].

Progress Tracker акумулює взаємодії користувача для формування детальної аналітики. Система зберігання даних (Analytics Storage) оптимізована для роботи з часовими рядами, забезпечує цілісність даних, підтримує версійність контенту та масштабування.

Типовий сценарій взаємодії демонструє повний цикл обробки запиту користувача: від розпізнавання наміру до формування відповіді, оцінювання, оновлення профілю та вибору наступного завдання: Frontend передає повідомлення до Chatbot Controller через HTTPS POST; контролер відправляє текст до NLP Engine для аналізу (intent: grammar_question, topic: present_perfect, level: B1); запитує User Profile Manager для контексту (weak_areas: [present_perfect]); звертається до Learning Module Manager, який отримує з Content Repository пояснення та приклади для рівня B1; контролер агрегує результати у coherent response з інтерактивною кнопкою; логує взаємодію до Progress Tracker → Analytics Storage; надсилає JSON response до Frontend. При оцінюванні відповіді Feedback Analyzer перевіряє correctness, валідує граматику, логує результат до Progress Tracker, оновлює Learner Model через User Profile Manager та запитує наступну активність від Learning Module Manager.

Запропонована архітектура інтелектуального чат-бота для навчання англійської мови поєднує сучасні NLP-технології, машинного навчання та педагогічного дизайну в єдину функціональну систему. Вона забезпечує гнучке, персоналізоване та масштабоване навчальне середовище, здатне адаптуватися до індивідуальних потреб користувача. Ключові переваги поєднують модульність з незалежним розвитком компонентів, горизонтальну масштабованість для зростаючого навантаження, повну персоналізацію через інтеграцію моделі навчання (Learner Model), оптимізацію навчального процесу на основі даних та розширюваність для додавання нових функцій без реструктуризації.

Список використаної літератури:

1. Devlin J., Chang M., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. *Proceedings of NAACL-HLT 2019*. P. 4171-4186. DOI: https://doi.org/10.18653/v1/N19-1423
2. Rohrer D., Taylor K. The shuffling of mathematics problems improves learning. *Instructional Science*. 2007. Vol. 35. P. 481-498. DOI: https://doi.org/10.1007/s11251-007-9015-8

3. Kuhail M., Alturki N., Alramlawi S., Alhejori Kh. Interacting with educational chatbots: A systematic review. *Education and Information Technologies*. 2023. Vol. 28. P. 1-46. DOI: https://doi.org/10.1007/s10639-022-11177-3

Ключові слова: інтелектуальні освітні агенти, чат-бот, обробка природної мови, трансформерна модель, персоналізоване навчання
Keywords: intelligent educational agents, chatbot, natural language processing, transformer model, personalized learning

РОЗРОБКА ОСВІТНЬОГО МОДУЛЯ «ОРГАНІЗАЦІЯ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ ЗА ІНТЕРФЕЙСОМ OPENMP»

Чикунов Павло
кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», доцент

Богун Валентин
магістрант Бахмутського навчально-наукового професійно-педагогічного інституту Харківського національного університету імені В. Н. Каразіна

У інформаційній освіті важливе місце посідають дисципліни, спрямовані на формування у здобувачів компетентностей із організації високопродуктивних обчислень. Серед інструментарію, що використовується для практичної реалізації цього напряму на мовах C/C++, одним із найзручніших є відкритий стандарт паралельного програмування OpenMP [1].

Метою роботи є представлення досвіду організації освітнього модуля «Організація паралельних обчислень за інтерфейсом OpenMP» та опис змісту лабораторних робіт, спрямованих на поступове оволодіння базовими директивами OpenMP і методами аналізу ефективності паралельних програм.

Згідно з положеннями European HPC Competence Framework [2], фахівець у галузі паралельних обчислень повинен мати системні знання про архітектуру багатоядерних процесорів, особливості пам’яті, принципи багатопотоковості та оптимізації коду, а також практичний досвід програмування з використанням інтерфейсів OpenMP, MPI, CUDA чи SYCL.

Проведений SWOT-аналіз силабусів освітніх компонент провідних українських університетів засвідчив їх високий рівень, зокрема через використання технологій OpenMP, MPI та CUDA, проте виявив відсутність педагогічно орієнтованих підходів до викладання цих тем. У програмах спостерігається переважання технічної складової над методичною, недостатня деталізація лабораторних завдань, орієнтованих на формування дидактичних компетентностей, а також нерівномірність охоплення окремих технологій. Встановлено, що підготовка студентів потребує не лише

ознайомлення з теоретичними основами паралельного програмування, а й формування практичних навичок застосування сучасних засобів OpenMP у розв'язанні задач обробки великих даних. Для досягнення зазначеної мети авторами розроблено освітній модуль, що складається з чотирьох нових лабораторних робіт:

1. «Введення у OpenMP» – присвячена базовим директивам parallel та for, особливостям створення багатопотокових програм та порівнянню часу виконання послідовної й паралельної реалізацій;

2. «Дослідження стратегій планування у OpenMP» – зосереджується на аналізі впливу типів планування (static, dynamic, guided) на балансування навантаження між потоками;

3. «Критичні секції, атомарні операції та змагання потоків» – висвітлює засоби уникнення конфліктів доступу до спільних ресурсів за допомогою директив critical та atomic;

4. «Паралельна редукція та колективні обчислення» – демонструє використання директиви reduction для обчислення сум, мінімумів і максимумів без явної синхронізації.

Запропонований перелік лабораторних робіт обґрунтовано логікою поетапного формування у здобувачів компетентностей з організації паралельних обчислень за інтерфейсом OpenMP. Така послідовність забезпечує цілісність навчального процесу, поступове ускладнення змісту та набуття студентами практичних навичок, необхідних для професійної діяльності у сфері цифрових технологій і високопродуктивних обчислень.

Структура лабораторних робіт побудована за єдиним методичним принципом і включає вступ, теоретичні відомості, завдання для самостійного виконання, контрольні запитання та приклади очікуваних результатів. Такий підхід забезпечує логічну послідовність засвоєння матеріалу – від розуміння основних директив OpenMP до аналізу продуктивності програм та узагальнення отриманих результатів. Студенти знайомляться з призначенням директив і принципами їх дії, далі виконують практичні експерименти, після чого формулюють висновки щодо ефективності різних стратегій паралелізації. Завдяки цьому лабораторні роботи сприяють розвитку вмінь аналітичного мислення, дослідницької самостійності та навичок оцінювання швидкодії програм у багатопроцесорних середовищах.

Розроблено індивідуальні варіанти лабораторного практикуму, що реалізують практико-орієнтований підхід до вивчення OpenMP. Кожен варіант передбачає створення паралельної програми для розв'язання конкретної математичної або алгоритмічної задачі – від класичних методів пошуку простих чисел (решето Ератосфена, Сундарама, Аткіна, сегментоване решето) до використання сучасних тестів перевірки простоти (Ферма, Міллера-Рабіна, Люка-Лемера, Соловея-Штрассена, Агравала-Каяла-Саксени). Така

варіативність забезпечує поступове ускладнення завдань, дозволяє студентам дослідити різні моделі паралельних обчислень, порівняти ефективність алгоритмів і сформувати вміння оптимізувати програми під архітектуру багатоядерних систем.

Результати практичних експериментів, передбачених лабораторним практикумом, наочно демонструють студентам істотне прискорення обчислень порівняно з послідовним виконанням програм. Поєднання теоретичних знань та практичних експериментів створює основу для розвитку критичного мислення.

Висновки. Впровадження освітнього модуля у навчальний процес дозволило підвищити якість засвоєння матеріалу, мотивацію до дослідницької діяльності та формування базових компетентностей у сфері паралельних обчислень.

Список використаної літератури:

1. OpenMP Architecture Review Board. OpenMP Application Programming Interface. Version 5.2. Nov 2021.
2. European High-Performance Computing Joint Undertaking (EuroHPC JU). European HPC Competence Framework. Luxembourg: Publications Office of the EU, 2022.

Ключові слова: OpenMP, паралельні обчислення, лабораторні роботи, C++.
Keywords: OpenMP, parallel computing, laboratory work, C++.

ДОСЛІДЖЕННЯ СПЕКТРАЛЬНОЇ ДЕГРАДАЦІЇ СЕЛЕКТИВНОСТІ БІНАРНИХ КОДОВИХ СЛІВ ПРИ МАСШТАБУВАННІ

Баландіна Наталія

Національний університет «Одеська юридична академія»,
старший викладач кафедри кібербезпеки

Однією із сучасних концепцій побудови стеганографічних методів є концепція кодового управління [1], яка дозволяє створювати методи, що працюють у часовій області. Це забезпечує не лише мінімальні витрати обчислювальних ресурсів на вбудовування додаткової інформації, а й високий рівень стійкості до атак, спрямованих на виявлення або знищення прихованого повідомлення, надійність його сприйняття, а також підвищену пропускну спроможність каналу.

Ядром таких методів є кодові слова, які в них застосовуються та повністю визначають їх характеристики. Саме конкретний вид кодового слова визначає у яку частотну складову буде виконано вбудовування додаткової інформації, та наскільки цілеспрямованим буде цей вплив. У роботі [2] було докладно досліджено механізми побудови кодових слів для кодового

управління та введено показники енергії E та селективності κ кодового слова $T = \|t_{ij}\|, i, j = 1,2,...,\mu$ розміру $\mu \times \mu$, які визначаються як

$$E = \sum_{i=1}^{\mu}\sum_{j=1}^{\mu} t_{i,j}^2, \quad \kappa = \frac{|s_{k,l}|}{\sum_{i=1}^{\mu}\sum_{j=1}^{\mu}|s_{i,j}|}, \tag{1}$$

де $s_{i,j}, i, j = 1,2,...,\mu$ — трансформанти дискретного косинусного перетворення (ДКП) кодового слова T, k,l — індекси по рядкам і стовбцям трансформанти ДКП, на яку зосереджено вплив кодового слова T.

Особливо важливим є коефіцієнт селективності кодового слова, який показує наскільки цілеспрямованим є вплив кодового слова на задану трансформанту ДКП, а отже наскільки воно є здатним забезпечити саме необхідні властивості результуючого стеганоповідомлення.

У роботі [2] також показано, що для кодових слів, що впливають на найбільш практично цінну трансформанту ДКП (2,1), які забезпечують найбільшу стійкість до атак проти вбудованого повідомлення, коефіцієнт селективності κ суттєво знижується із зростанням розміру кодового слова μ. Проте глибинні причини такого зменшення потребують подальшого дослідження. Зокрема, невизначеними залишаються спектральні компоненти, які виступають акцепторами енергії, що призводить до зниження селективності з ростом довжини кодового слова.

Метою цієї роботи є дослідження особливостей змін коефіцієнта селективності кодових слів (на прикладі кодового слова, що впливає на трансформанту ДКП (2,1)) при зростанні їх довжини.

Розглянемо кодове слово $T_{4,(1,2)}$, що забезпечує вплив на трансформанту ДКП (2,1) у просторовій області, а також його трансформанти ДКП

$$T_{4,(1,2)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \end{bmatrix}, \; C_{T_{4,(1,2)}} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 3.6955 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1.5307 & 0 & 0 & 0 \end{bmatrix}. \tag{2}$$

Таким чином, згідно до (1) коефіцієнт селективності цього кодового слова дорівнює $\kappa = 0.7071$, що за його фізичним трактуванням означає, що 70.71% енергії кодового слова витрачається на зміну трансформанти ДКП (2,1), тоді як інші 29.29% витрачаються на зміну трансформанти ДКП (4,1).

Отримана селективність є недостатньою. Принципово можливо досягнути підвищення селективності за рахунок використання недвійкових кодових слів [2]. Однак подібний підхід пов’язаний із зниженням надійності сприйняття, оскільки недвійкова структура вимагає більшого збурення пікселів контейнера.

Отже, розподіл енергії кодового слова із зростанням його довжини потребує більш пильного дослідження, результати якого показані у табл. 1, та подальшого переосмислення. У табл. 1 показані трансформанти ДКП, що зазнають збурення від застосування кодових слів $T_{4,(1,2)}$, $T_{8,(1,2)}$, $T_{16,(1,2)}$ розмірів 4×4, 8×8 та 16×16, які націлені на трансформанту ДКП (2,1), число змін знаку η функції ДКП, що відповідає даній трансформанті (характеристика частоти трансформанти) та відсоток зміни від загального рівня змін трансформант ДКП.

Таблиця 1 — Розподіл енергії кодового слова по трансформантам ДКП із зміною його довжини

$\mu=4,\ \kappa=0.7071$								
$s_{i,j}$	(2,1)				(4,1)			
Значення	3.6955				-1.5307			
η	1				3			
%	70.71				29.29			
$\mu=8,\ \kappa=0.5603$								
$s_{i,j}$	(2,1)		(4,1)		(6,1)		(8,1)	
Значення	7.2490		-2.5455		1.7009		-1.4419	
η	1		3		5		7	
%	56.03%		19.68%		13.15%		11.15%	
$\mu=16,\ \kappa=0.4675$								
$s_{i,j}$	(2,1)	(4,1)	(6,1)	(8,1)	(10,1)	(12,1)	(14,1)	(16,1)
Значення	14.4282	-4.8718	3	-2.2292	1.8295	-1.6036	1.4778	-1.4211
η	1	3	5	7	9	11	13	15
%	46.75%	15.79%	9.72%	7.22%	5.93%	5.2%	4.79%	4.6%

На підставі результатів, наведених у табл. 1, можна зробити важливі висновки щодо впливу довжини кодового слова на його селективність у контексті побудови стеганографічних методів на основі кодового управління. Згідно із отриманими результатами, зі зростанням довжини кодового слова спостерігається поступове зниження коефіцієнта селективності, що виражається у дедалі меншій частці енергії, спрямованій на цільову трансформанту ДКП (2,1). Якщо для короткого кодового слова понад 70% енергії зосереджується саме на цій трансформанті, то при довжині $\mu=16$ ця частка знижується до менше ніж 47%, тоді як решта енергії розподіляється між трансформантами вищих порядків.

На перший погляд, така динаміка може здаватися наслідком простого «розсіювання» енергії по зростаючій кількості частотних компонент. Проте справжня причина є глибшою та пов’язана з природою частотного простору,

що формується під час дискретного косинусного перетворення. Збільшення довжини кодового слова фактично змінює спектральну роздільну здатність: трансформанти, що з'являються у блоках більшого розміру, не є продовженням або деталізацією тих, що були у менших блоках — вони мають іншу частотну сутність.

Таким чином, коли кодове слово великої довжини впливає на трансформанту (2,1) у великому блоці, воно одночасно збурює низку інших трансформант, які мають свою частотну природу. Це означає, що зростає не лише кількість збурених компонент, а й зменшується можливість сконцентрувати вплив саме на цільовій частоті, яка в умовах конкретної стеганографічної моделі є найбільш стійкою або малопомітною. У цьому контексті слід говорити не лише про енергетичне, але і про спектрально-інформаційне ослаблення селективності. Воно полягає в тому, що кодове слово втрачає здатність точно й фокусовано передавати інформацію через обраний частотний канал, що є однією з головних переваг концепції кодового управління. Тобто, окрім кількісного зменшення впливу на цільову трансформанту, із зростанням розміру кодового слова відбувається також якісна втрата здатності управляти спектральним профілем стеганоповідомлення, що прямо впливає на його стійкість, надійність сприйняття і пропускну спроможність.

Усе вищесказане дозволяє дійти до важливого висновку: ефективність концепції кодового управління із використанням найбільш ефективних кодових слів, наприклад, тих, що впливають на трансфоманту ДКП (2,1), може помітно знижуватись зі зростанням їх розміру. З одного боку, більша довжина дозволяє отримати кращу захищеність, однак з іншого — призводить до втрати контрольованості над частотним вбудовуванням. Таким чином, для випадку довших кодових слів концепція кодового управління потребує удосконалення для збереження високого рівеня селективності при масштабуванні методу.

Список використаної літератури:

1. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. Problemele energeticii regionale. 2021. No. 4 (52). P. 115-130.
2. Kobozeva A.A., Sokolov A.V. Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method. Radiotekhnika. 2021. 4 (207). P. 27–39.

Ключові слова: стеганографія, математичні основи, селективність, дискретне косинусне перетворення (ДКП), спектральний аналіз.
Keywords: steganography, mathematical foundations, selectivity, discrete cosine transform (DCT), spectral analysis.

МЕТОДИ АНАЛІЗУ ДАНИХ У ПРОГНОЗУВАННІ ПОПИТУ НА ТОВАРИ ЕКТРОННОЇ КОМЕРЦІЇ

Лобода Юлія

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат педагогічних наук, доцент

Дроздов Богдан

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Прогнозування попиту в електронній комерції є одним із ключових завдань, що визначає ефективність управління запасами, планування логістики та формування маркетингових стратегій. На відміну від традиційного ритейлу, дані електронної комерції характеризуються більшою мінливістю та багатофакторністю: на обсяги продажів впливають сезонні коливання, рекламні кампанії, поведінка користувачів на сайті, відгуки, динаміка цін, а також зовнішні фактори від глобальних трендів до соціальної активності в мережі. Тому застосування сучасних методів аналізу даних, здатних працювати з великими, різнорідними та швидкозмінними наборами інформації, стає особливо актуальним.

У науковій літературі виокремлюють кілька основних груп методів, що застосовуються для прогнозування попиту. Традиційні статистичні підходи, такі як ARIMA, SARIMA та моделі експоненціального згладжування, залишаються актуальними для відносно стабільних часових рядів. Вони тоді, коли структура попиту є сталою, а вплив зовнішніх факторів обмежений. Проте у випадку складних, нестабільних або високоволатильних даних точність цих методів істотно зменшується, що підтверджено сучасними дослідженнями [1, 2].

Зі зростанням обсягів даних дедалі ширшого застосування набувають методи машинного навчання, які здатні моделювати нелінійні залежності та взаємодію великої кількості параметрів. До таких підходів належать Random Forest, Gradient Boosting, XGBoost та LightGBM. Вони демонструють високу точність на значних масивах даних, особливо коли необхідно враховувати ціну товару, кількість переглядів, інтенсивність маркетингових активностей або сезонні патерни. За результатами досліджень доведено, що градієнтні бустингові алгоритми забезпечують суттєве зменшення помилки порівняно з класичними статистичними моделями [3, 4].

Подальший розвиток методів прогнозування попиту пов’язаний із впровадженням моделей глибинного навчання. Рекурентні нейронні мережі здатні враховувати довготривалі часові залежності, що робить їх ефективними для роботи зі складними та шумними часовими рядами,

характерними для продажів на рівні окремих SKU [3]. Використання таких моделей суттєво підвищує точність прогнозів, особливо коли попит формується під впливом великої кількості взаємопов'язаних факторів.

Окремо уваги заслуговує розвиток мультимодальних та гібридних моделей, які поєднують дані різної природи – історію продажів, поведінкові характеристики користувачів, текстові відгуки, візуальні ознаки товарів та інформацію про маркетингові події. Поєднання часових моделей з методами оброблення природної мови, зокрема BERT або аналізом емоційних відгуків, дає змогу враховувати соціальні та семантичні сигнали, які раніше не охоплювали класичні методи [4, 5].

Важливу роль відіграють технології оброблення великих даних, які забезпечують аналіз значних обсягів інформації у режимі близькому до реального часу. Платформи Hadoop та Apache Spark дозволяють моделювати попит у масштабі великих маркетплейсів, де щоденно накопичуються мільйони нових транзакцій. Це забезпечує гнучкість системи та дає змогу швидко оновлювати моделі, що є критично важливим під час розпродажів із різким зростанням попиту та в умовах нестабільної ринкової ситуації.

Сучасні дослідження підтверджують, що жоден окремий підхід не є універсальним для всіх товарних категорій. У практиці електронної комерції застосовують комбінації статистичних методів, алгоритмів машинного та глибинного навчання, а також мультимодальні моделі, які враховують широкий спектр впливових чинників. Унаслідок цього розвиток прогнозування попиту рухається у напрямі створення гібридних моделей, інтеграції різнорідних даних та формування масштабованих інтелектуальних систем.

Список використаної літератури:

1. Karthika D., Karthikeyan K. A Recent Review Article on Demand Forecasting. *Journal of Xi'an University of Architecture & Technology*. 2020, Vol. 12, Iss. 3, pp. 5769-5777. https://www.researchgate.net/publication/354726783
2. Filahi Y., Gul O., Elghirani A. et al. (2025) Enhanced E-commerce decision-making through sentiment analysis using machine learning-based approaches and IoT. *PLoS One*. 2025, Vol. 20(6). https://doi.org/10.1371/journal.pone.0326744.
3. Zohdi M., Rafiee M., Kayvanfar V. et al. Demand forecasting based machine learning algorithms on customer information: an applied approach. *Int. j. inf. tecnol*. 2022, 14, pp. 1937–1947. https://doi.org/10.1007/s41870-022-00875-3.
4. Trang Ho, Tran Ly, Hieu M. Machine Learning in Demand Forecasting. *International Research Journal of Advanced Engineering and Science*. Vol. 7, Issue 3, pp. 225-233, 2022. https://www.researchgate.net/publication/370155418_ Machine_Learning_in_Demand_Forecasting
5. Weiwei Cai, Yaping Song. Multimodal Data Guided Spatial Feature Fusion and Grouping Strategy for E-Commerce Commodity Demand Forecasting. *Mobile Information Systems*. 2021, 14 p. https://doi.org/10.1155/2021/5568208

Ключові слова: електронна комерція, прогнозування попиту, аналіз даних, машинне навчання, глибинне навчання, часові ряди, мультимодальні моделі, великі дані.
Keywords: e-commerce, demand forecasting, data analysis, machine learning, deep learning, time series, multimodal models, big data.

МУЛЬТИМЕДІЙНІ СИСТЕМИ ДЛЯ МОНІТОРИНГУ ТА АНАЛІЗУ КОНТЕНТУ ВІДЕОПЛАТФОРМ

Задерейко Олександр
доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Барбенягре Валерія
студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Мультимедійні системи для моніторингу та аналізу відеоплатформ посідають важливе місце в сучасному інформаційному просторі. Стрімкий розвиток технологій, зростання кількості користувачів інтернету та популярність відеоконтенту зумовлюють потребу в ефективних інструментах для збору, обробки та аналізу мультимедійних даних. Сучасні відеоплатформи, такі як YouTube, TikTok, Vimeo чи Twitch, виконують не лише роль засобу поширення інформації, а й виступають потужними аналітичними системами, що впливають на формування суспільної думки, освітніх процесів та бізнесу [1].

Мультимедійні системи - це комплекс апаратних та програмних засобів, що забезпечують створення, обробку, зберігання й відтворення аудіовізуальної інформації [2]. Їх основна мета - забезпечити можливість інтеграції різних типів медіа у єдине середовище. Для відеоплатформ такі системи є базовими, адже дозволяють реалізовувати зручний пошук контенту, налаштування рекомендацій і персоналізацію користувацького досвіду.

Одним із ключових напрямів розвитку мультимедійних систем є впровадження технологій штучного інтелекту та машинного навчання. Завдяки цим технологіям здійснюється автоматичний аналіз мультимедійного контенту: розпізнавання обличчя людини, її емоцій та мови. Це дозволяє фільтрувати заборонений або небажаний контент, виявляти недостовірну маніпулятивну інформацію, а також створювати набір рекомендацій, які підвищують залученість користувачів [3]. Наприклад, алгоритми YouTube

враховують тривалість перегляду, кількість взаємодій і навіть тематику коментарів для визначення релевантності відеоконтенту [4].

Мультимедійні системи активно використовуються для моніторингу якості відеопотоків. Вони аналізують технічні параметри трансляцій, стабільність сигналу, швидкість передавання даних і рівень стиснення, що впливає на якість відтворення відео. Такі системи дають змогу підтримувати високий рівень користувацького досвіду навіть при великому навантаженні на сервери. Важливу роль у цьому відіграють хмарні технології, які забезпечують масштабованість, безперебійність роботи та збереження великих обсягів відеоінформації [5].

Сучасні дослідження підтверджують, що системи моніторингу відеоплатформ переходять на рівень «розумного» аналізу потоків даних. Вони здатні виявляти погіршення якості трансляцій у реальному часі, прогнозувати технічні проблеми й автоматично оптимізувати ресурси. Такі рішення вже застосовуються провідними компаніями у сфері медіааналітики, які використовують хмарні сервіси для виявлення технічних помилок у потоковому відео та покращення стабільності контенту. Крім того, мультимедійні системи дедалі частіше інтегруються з платформами для збору метаданих - переглядів, взаємодій користувачів, географії трафіку, що дозволяє формувати комплексні аналітичні звіти та приймати рішення на основі даних.

Значення мультимедійних систем простежується у галузі освіти. Відеоплатформи все частіше використовуються як засіб дистанційного навчання. Мультимедійні системи дають можливість викладачам відстежувати активність студентів, визначати ступінь засвоєння матеріалу, а також аналізувати ефективність поданого навчального відеоконтенту. Завдяки цьому формується нова модель освітнього процесу, орієнтована на інтерактивність і гнучкість [6].

У системах онлайн-освіти важливу роль відіграє аналітика поведінки користувачів - час перегляду, частота повторних переглядів, взаємодія з навчальними відео. Такі показники дозволяють оптимізувати навчальний контент і створювати більш ефективні освітні програми.

Не менш важливим є застосування мультимедійних систем у сфері інформаційної безпеки. Відеоплатформи часто стають об’єктами кібератак, що спрямовані на викрадення даних користувачів або поширення дезінформації. Системи моніторингу дозволяють своєчасно виявляти загрози, відстежувати підозрілу активність та захищати персональні дані. Технології кібербезпеки, зокрема шифрування даних і багаторівнева автентифікація, забезпечують безпечну взаємодію користувачів із платформами.

Крім цього, сучасні мультимедійні системи здатні здійснювати аналіз достовірності відеоконтенту, виявляючи спроби маніпуляцій чи фальсифікацій. Це особливо актуально в умовах розвитку технологій deep-fake, які дозволяють створювати підроблені відео високої якості. Використання алгоритмів машинного зору та аналізу цифрових відбитків відеофайлів допомагає підвищити рівень довіри до інформації, що поширюється через відеоплатформи.

Крім того, мультимедійні системи сприяють розвитку креативних індустрій. Інструменти для аналітики та моніторингу відеоплатформ допомагають авторам контенту оцінювати популярність своїх робіт, визначати теми, що викликають найбільший інтерес, і вдосконалювати власний творчий підхід. Це створює передумови для появи якісного, соціально значущого контенту, який поєднує розважальну, освітню та культурну складові. Таким чином, мультимедійні технології не лише підтримують технічне функціонування відеоплатформ, а й формують нову культуру цифрового споживання медіа, засновану на аналітиці, інноваціях та взаємодії.

Висновки. Отже, мультимедійні системи для моніторингу та аналізу відеоплатформ є невід'ємною складовою сучасної цифрової екосистеми. Вони поєднують технології обробки відео, штучного інтелекту, великих даних та кібербезпеки, забезпечуючи якісну взаємодію між користувачем і медіа-ресурсом. Їх подальший розвиток сприятиме підвищенню ефективності роботи онлайн-платформ, покращенню якості контенту та формуванню безпечного інформаційного простору. Таким чином, мультимедійні системи виступають ключовим елементом інфраструктури майбутнього, що визначає рівень розвитку цифрового суспільства та культури споживання медіаінформації.

Список використаних джерел:

1. Wave.video - Що таке відеоплатформа і навіщо вона потрібна. URL: https://wave.video/ua/blog/video-platform/
2. Педагогічні науки - Сучасні мультимедійні технології в освітньому процесі. URL: https://pednauk.cusu.edu.ua/index.php/pednauk/article/view/1476
3. AIN.UA - Штучний інтелект у відеоаналітиці. URL: https://ain.ua/2024/04/12/shtuchnyj-intelekt-u-videoanalizy/
4. Google Support - Як працює алгоритм YouTube. URL: https://support.google.com/youtube/answer/6342839?hl=uk
5. DOU.UA - Хмарні технології та відеосервіси. URL: https://dou.ua/forums/topic/42020/
6. Укрінформ - Кібербезпека України: шляхи розвитку та можливості. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html

Ключові слова: генеративний ШІ.
Keywords: generative AI.

АНАЛІЗ СУЧАСНИХ МЕХАНІЗМІВ ЗАХИСТУ ВІД АТАК НА ВИЯВЛЕННЯ НАЛЕЖНОСТІ

Хоменко Ігор

аспірант кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут»

Широке впровадження машинного навчання (ML та великих мовних моделей (LLM), які навчаються на величезних наборах даних, що часто містять конфіденційну або приватну інформацію, додало нові вектори атак та загрози для приватності. Однією з фундаментальних загроз є атаки на визначення належності (Membership Inference Attack), під час яких зловмисник намагається встановити, чи був конкретний запис використаний у навчальному наборі моделей. Наприклад, якщо зловмисник визначить, що медичний запис пацієнта був використаних для навчання моделі прогнозування захворювань, це розкриє діагнози пацієнта. Успішна атака на визначення належності може мати критичні наслідки та завдати значні фінансові збитки [1].

Метою даного дослідження є проведення комплексного аналізу атак на визначення належності на сучасні системи штучного інтелекту, серед яких є великі мовні моделі, які впроваджуються у всі галузі нашого життя. Дослідження має на меті ідентифікувати та оцінити ефективність різноманітних векторів атак, а також проаналізувати відповідні механізми та методи захисту [2]. Під час дослідження було проведено систематичний огляд та аналіз ключових наукових праць, технічних звітів та виконано експеримент за допомогою llm-jp-membership-inference на ресурсі Hugging Face, що надає віртуальну машину і мовні моделі для експериментів [3].

Проведене дослідження дозволило виявити та кількісно оцінити ключові аспекти витоку інформації про належність у різних парадигмах машиного навчання. Зловмисник навчає модель атаки (класифікатор), використовуючи вектори передбачень (prediction vectors) або значення впевненості (confidence values) цільової моделі. Модель атаки розрізняє поведінку цільової моделі на вхідних даних, використаних для її навчання (in), та даних, які вона не бачила і прогнозує (out). Для навчання моделі атаки часто використовується метод тіньоового навчання (shadow training), де створюються допоміжні тіньові моделі зі схожою архітектурою та розподілом даних. Результати підтверджують, що успіх MIA прямо пов’язаний зі ступенем перенавчання цільової моделі. Якщо модель схильна до перенавчання (тобто демонструє високу точність на навчальному наборі, але низьку на тестовому), вона випускає більше інформації про свої навчальні вхідні дані [3].

Захисні стратегії проти атак на виявлення належності варіюються залежно від середовища навчання та цілей, які вони переслідують, часто вимагаючи компромісу між точністю та приватністю. Середовища можуть бути

типу Централізованого навчання (CL), федеративного навчання (FL) та доналаштування (Fine-Tuning LLM). Порівняльний аналіз захисних методів наведений у Таблиці 1 на основі тестування за допомогою репозиторію llm-jp-membership-inference та технічних звітів інших методів захисту [4].

Сутність методу Диференціальної приватності (DP) полягає у введенні ретельно каліброваного шуму в чутливі дані, градієнти або параметри моделі. Це є "легкою" технікою, що забезпечує строгий захист приватності, обмежуючи розбіжність між ймовірністю отримання результату, коли індивідуальний зразок включено до навчального набору, і коли його виключено. Завдяки такій конструкції, моделі, захищені DP, за визначенням є стійкими до атак на виявлення належності (MIA) [6].

Механізм регуляризації є однією з ключових стратегій захисту проти атак на виявлення належності (MIA), оскільки він безпосередньо спрямований на усунення основної причини витоку приватності — перенавчання (overfitting) моделі [7]. Регуляризація ефективно захищає від MIA, оскільки вона прагне зменшити рівень перенавчання моделей машинного навчання, що обмежує їхню прогностичну силу та узагальнювальну здатність. Моделі з гарною регуляризацією повинні мінімізувати витік інформації про свої навчальні дані, і атака MIA може використовуватися як метрика для кількісної оцінки цього рівня захисту. Регуляризаційні методи прагнуть зменшити розрив в узагальненні (generalization gap), тим самим знижуючи вразливість до MIA [8].

Обфускація вихідних даних (або пертурбація вихідних даних) є механізмом захисту, який застосовується на фазі висновку (inference) моделі. Основною метою цього підходу є зменшення кількості інформації, яку зловмисник може отримати з прогнозованого вектору ймовірностей (prediction vector) цільової моделі, щоб ускладнити проведення атаки MIA. Цей механізм є пост-процесинговим методом, який використовується для узгодження вихідних даних моделі між навчальними та тестовими зразками[9].

Селективна обфускація даних (SOFT) є інноваційним механізмом захисту, спеціально розробленим для мінімізації витоку приватності під час тонкого налаштування великих мовних моделей [10]. Суть методу полягає у використанні селективного вибору впливових даних для зменшення ризику атак на виявлення належності. SOFT реалізується шляхом заміни найбільш вразливих зразків у наборі даних для тонкого налаштування на обфусковані парафрази [11].

Основний принцип Безпечної агрегації (Secure Aggregation) полягає у запобіганні витоку інформації шляхом обміну зашифрованими оновленнями моделі замість відкритих [12]. SecAgg, зокрема, використовує методи розподілу секретів (secret sharing) та подвійного маскування. Це забезпечує, що центральний сервер не має доступу до індивідуальних локальних оновлень моделей клієнтів. Завдяки цьому, центральний агрегатор може обчислити

лише суму або середнє значення оновлень, отримуючи знання виключно про агреговану модель [13].

Часткове спільне використання є стратегією захисту у федеративному навчанні, головна мета якої — зменшити ефективність атак на виявлення належності (MIA) шляхом придушення або обмеження обсягу інформації, якою обмінюються під час комунікаційної фази. Цей підхід зменшує обсяг даних, доступних зловмисникам, обмежуючи обмін параметрами або градієнтами моделі [15].

Таблиця 1. Порівняльний аналіз захисних механізмів проти MIA

№	Механізм захисту	Контекст	Захист	Фаза Застосування
1	Диференційна приватність	CL/FL	Додавання шуму до даних, градієнтів або параметрів моделі. Забезпечує строгі теоретичні гарантії приватності	Навчання
2	Регуляризація (L2 або Dropout)	CL	Зменшення перенавчання (overfitting), яке є основною причиною витоку належності	Навчання
3	Обфускація вихідних даних (Output Perturbation)	CL	Округлення точності вектора прогнозування або обмеження вихідних даних моделі до k найбільш імовірних класів	Висновок
4	Дистиляція знань (Knowledge Distillation)	CL	Передача знань від більшої моделі-вчителя до меншої моделі-учениці, що сприяє кращому узагальненню та зниженню перенавчання	Навчання
5	Селективна обфускація даних	Fine-tun-ing LLM	Виявлення та заміна найбільш впливових/вразливих зразків навчального набору семантично еквівалентними парафразами	Навчання
6	Безпечна агрегація	FL	Використання криптографічних методів (наприклад, Secret Sharing) для забезпечення того, що центральний сервер бачить лише агрегований результат, а не індивідуальні оновлення клієнтів	Комунікація та агрегація
7	Часткове спільне використання	FL	Приховування певних оновлень моделі (наприклад, селективний градієнт) для зменшення ефективності атак	Комунікація

Аналіз поточних механізмів захисту від атак на виявлення належності (MIA) демонструє, що всі вони оперують у складному полі компромісів між

конфіденційністю (privacy), функціональною корисністю моделі (utility) та обчислювальною ефективністю. Жоден з існуючих методів не забезпечує універсального, бездоганного захисту без певних обмежень. Хоча DP є золотим стандартом, оскільки надає строгі теоретичні гарантії захисту від MIA, її впровадження неминуче призводить до суттєвої втрати корисності моделі. Для досягнення надійного захисту (мале є) часто доводиться жертвувати точністю прогнозів. У федеративному навчанні (ФН), якщо кількість учасників невелика, додавання шуму може перешкоджати конвергенції глобальної моделі. Селективна обфускація даних (SOFT): Цей підхід є одним із найбільш збалансованих для захисту тонконастроєних ВММ. SOFT демонструє здатність значно знижувати успішність MIA (до рівня, близького до випадкового вгадування), при цьому мінімізуючи втрату корисності моделі. Його перевага полягає у селективній роботі з найбільш вразливими (впливовими) зразками, зменшуючи перенавчання моделі на їхніх точних формулюваннях через парафразування.

Подальші дослідження повинні бути спрямовані на розробку уніфікованих бенчмарків та комплексних механізмів, які зможуть одночасно забезпечувати високу приватність, корисність та ефективність.

Список використаної літератури:

1. Shokri R., Stronati M., Song C., Shmatikov V. Membership inference attacks against machine learning models. 2017 IEEE Symposium on Security and Privacy (SP). 2017. P. 3–18.
2. He J., Chen M., Gu Y., Chen K. Membership Inference Attacks on In-Context Learning Recommendation. Proceedings of the 17th ACM Conference on Recommender Systems (RecSys ’25). 2025. P. 1–12.
3. GitHub - Ihor-Khomenko/llm-jp-membership-inference: This is the repository for llm jp membership inference attack. GitHub. URL: https://github.com/Ihor-Khomenko/llm-jp-membership-inference (date of access: 01.11.2025).
4. Puerto H., Gubri M., Yun S., Oh S. J. Scaling Up Membership Inference: When and How Attacks Succeed on Large Language Models. arXiv preprint arXiv:2411.00154. 2024.
5. Zhang K., Cheng S., Guo H. et al. SOFT: Selective Data Obfuscation for Protecting LLM Fine-tuning against Membership Inference Attacks. arXiv preprint. 2024.
6. Meeus M., Shilov I., Jain S. et al. SoK: Membership Inference Attacks on LLMs are Rushing Nowhere (and How to Fix It). arXiv preprint arXiv:2406.17975. 2024.
7. Nasr M., Shokri R., Houmansadr A. Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning. 2019 IEEE Symposium on Security and Privacy (SP). 2019. P. 739–753
8. Dwork C. Differential privacy. Encyclopedia of Cryptography and Security. Springer, 2011. P. 338–340.

9. Carlini N., Tramer F., Wallace E. et al. Extracting Training Data from Large Language Models. 30th USENIX Security Symposium (USENIX Security 21). 2021. P. 2633–2650.
10. Yeom S., Giacomelli I., Fredrikson M., Jha S. Privacy risk in machine learning: Analyzing the connection to overfitting. 2018 IEEE 31st Computer Security Foundations Symposium (CSF). 2018. P. 268–282.
11. Hu H., Salcic Z., Sun L. et al. Membership Inference Attacks on Machine Learning: A Survey. ACM Computing Surveys (CSUR). Vol. 54, No. 11s. 2022. P. 1–37.
12. Duan M., Suri A., Mireshghallah N. et al. Do membership inference attacks work on large language models? arXiv preprint arXiv:2402.07841. 2024.
13. Maini P., Jia H., Papernot N., Dziedzic A. LLM Dataset Inference: Did you train on my dataset? arXiv preprint arXiv:2406.06443. 2024
14. Bonawitz K., Ivanov V., Kreuter B. et al. Practical secure aggregation for privacy-preserving machine learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017. P. 1175–1191.
15. Yuan W., Yang C., Nguyen Q. V. H. et al. Interaction-level Membership Inference Attack Against Federated Recommender Systems. Proceedings of the Web Conference 2023. 2023. P. 1–10.

Ключові слова: Атака на виявлення належності, Великі мовні моделі, приватність, захисні механізми.
Keywords: Membership Inference Attack, Large Language Models, Privacy, Defence Mechanisms

ВИЯВЛЕННЯ НЕТИПОВИХ ПОДІЙ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

Чикунов Павло

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», доцент

Флюнт Владислав

студент Національного університету «Одеська юридична академія»

Системи відеоспостереження є одним із інструментів моніторингу та забезпечення безпеки у громадських місцях, транспортних вузлах, промислових об’єктах, навчальних закладах і приватних структурах. Зі зростанням кількості камер та обсягу даних постає проблема оперативного аналізу відеопотоків. Оператор фізично не може відстежувати десятки джерел одночасно, тому автоматизовані системи відеоспостереження є критично необхідними.

Використання технологій штучного інтелекту дозволяє автоматизувати процеси виявлення нетипових або аномальних подій, таких як залишені предмети, поява людини у забороненій зоні, натовпова паніка, агресивна поведінка або порушення маршрутів руху. Ці події часто не піддаються формальному опису, що робить традиційні правило-орієнтовані методи

малоефективними. Актуальними є алгоритми машинного навчання, що здатні самостійно моделювати поняття аномальної поведінки без ручного налаштування правил.

Метою роботи є розроблення архітектури та створення прототипу системи автоматизованого виявлення нетипових подій у відеопотоках на основі глибинних нейронних мереж і GPU-прискорення.

Дослідження виявлення аномалій у відео активно розвиваються протягом останнього десятиліття. Автори роботи [1] запропонували використання конволюційного автоенкодера для навчання моделі «нормальної» поведінки. Автори роботи [2] удосконалили підхід через повнозгорткову нейромережу, що працює у реальному часі. У роботі [3] наведено результати реалізації ідеї прогнозування наступного кадра, визначаючи аномалії за відхиленням між очікуваним і фактичним відео. Дослідження [4] присвячено аналізу ефективності кластеризації патернів руху у комбінації з глибинними ознаками, а дослідники [5] запропонували підхід Continual Learning, що враховує зміну середовища.

Окрім академічних рішень, активно розвиваються комерційні системи. Avigilon UMD/UAD від Motorola Solutions впроваджує алгоритми автоматичного виявлення нетипових рухів без попереднього навчання на аномаліях. BriefCam інтегрує інструменти поведінкового аналізу та пошуку об’єктів у VMS Milestone XProtect. Irisity IRIS+ та Oosto Protect поєднують розпізнавання облич із поведінковими моделями. Axis Object Analytics реалізує базові rule-based сценарії на рівні edge-пристроїв.

SWOT-аналіз цих платформ показав, що комерційні рішення забезпечують стабільність і масштабованість, але мають обмежену можливість наукової модифікації алгоритмів; натомість відкриті бібліотеки (зокрема anomalib, OpenVINO, FiftyOne) дозволяють реалізувати академічні експерименти та дослідження на реальних наборах відео.

Для реалізації системи вибрано мову Python завдяки широкому набору бібліотек для комп’ютерного зору та глибинного навчання. До технологічного стеку програмної реалізації входять такі інструменти:

– OpenCV для захоплення та попередня обробка відеопотоку (нормалізація кадрів, фільтрація шумів, виявлення руху);

– PyTorch для побудови, навчання та інференсу нейромережевої моделі автоенкодера;

– TensorFlow для реалізації альтернативних архітектур (3D-CNN, Vision Transformer);

– NumPy / Pandas для обробки та статистичного аналізу наборів даних;

– Matplotlib / Seaborn для візуалізації результатів та графіків втрат;

– CUDA та cuDNN для апаратного прискорення обчислень на GPU.

Запропоновано таку структуру системи:

модуль попередньої обробки відео відповідає за формування потоків і підготовку кадрів для аналізу;

модуль виявлення аномалій реалізує навчання автоенкодера на звичайних даних і порівняння реконструкцій із вхідними кадрами;

модуль візуалізації та збереження результатів забезпечує відображення виявлених аномалій у відеопотоці й запис результатів у базу даних.

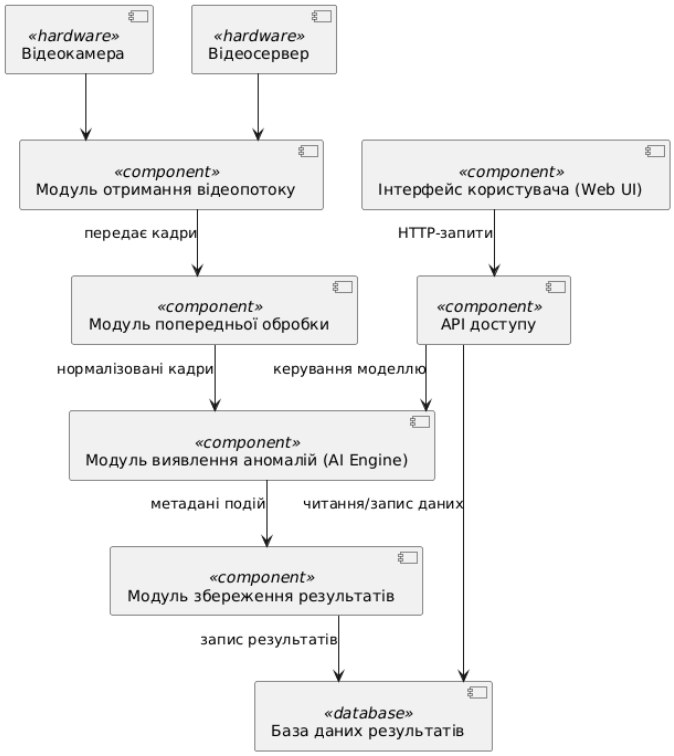

Рисунок 1 – Компонентна діаграма системи автоматизованого виявлення нетипових подій

Висновки. У роботі доведено актуальність застосування методів штучного інтелекту для автоматизованого виявлення нетипових подій у відеопотоках. Запропонована архітектура системи демонструє можливість побудови модульного рішення, яке поєднує попередню обробку відео, аналіз поведінкових ознак та візуалізацію виявлених подій. Подальший розвиток дослідження доцільно спрямувати на вдосконалення часових моделей, підвищення стійкості до змін середовища, зменшення кількості хибних спрацьовувань та інтеграцію рішення у більш складні інтелектуальні системи безпеки.

Список використаної літератури:

1. Hasan M., Choi J., Neumann J., Roy-Chowdhury A. K., Davis L. S. Learning Temporal Regularity in Video Sequences. IEEE CVPR, 2016.
2. Sabokrou M., Fathy M., Hoseini M., Klette R. Deep-Anomaly: Fully Convolutional Neural Network for Fast Anomaly Detection in Crowded Scenes. CVIU, 2018.
3. Liu W., Luo W., Lian D., Gao S. Future Frame Prediction for Anomaly Detection – A New Baseline. IEEE CVPR, 2018.

4. Ionescu R., Smeureanu S., Alexe B., Popescu M. Detecting Abnormal Events in Video Using Narrowed Normality Clusters. WACV, 2019.
5. Doshi K., Yilmaz Y. Continual Learning for Anomaly Detection in Surveillance Videos. IEEE Trans. Image Processing, 2021.

Ключові слова: відеоаналіз, аномальні події, штучний інтелект, нейронні мережі, автоенкодер, відеоспостереження.
Keywords: video analytics, anomaly detection, artificial intelligence, neural networks, autoencoder, surveillance.

АНАЛІЗ ТА РЕДИЗАЙН МОБІЛЬНОГО ЗАСТОСУНКУ НА ОСНОВІ UX-ДОСЛІДЖЕННЯ ТА ПРОТОТИПУВАННЯ

Селютін В'ячеслав

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Інтенсивний розвиток мобільних технологій та зростання частки користувачів, які взаємодіють із цифровими сервісами переважно через смартфони, актуалізує проблематику підвищення якості інтерфейсів мобільних застосунків. Сучасні дослідження у сфері human–computer interaction [1] показують, що ключовим чинником успішності мобільних продуктів є не лише функціональна повнота, але й оптимізований користувацький досвід, заснований на принципах когнітивної ергономіки, інформаційної архітектури та доступності [2].

Недостатня увага до юзабіліті часто призводить до збільшення когнітивного навантаження, дезорієнтації користувача, втрати мотивації до продовження роботи із застосунком. Актуальність дослідження полягає у необхідності комплексної оцінки інтерфейсу з позиції сучасних стандартів UX/UI, зокрема принципів людиноорієнтованого дизайну, дизайн-систем, моделювання сценаріїв поведінки та валідації користувацьких рішень через прототипування [3].

Мета дослідження полягає у розробленні оновленої концепції інтерфейсу мобільного застосунку шляхом проведення структурованого UX-аналізу, визначення проблем взаємодії та формування дизайн-системи, що забезпечує цілісність та відтворюваність інтерфейсних рішень.

Комплексний аналіз інтерфейсу виявив низку факторів, що потребують удосконалення. Встановлено порушення принципів візуальної ієрархії через нерівномірний розподіл акцентів, конкуренцію елементів за увагу та відсутність чіткої структури між основними та допоміжними діями. Виявлено нелогічну інформаційну архітектуру, що проявляється у дублюванні функціональних модулів у різних частинах інтерфейсу, фрагментованості шляхів взаємодії та недостатній передбачуваності навігації. Зафіксовано недотримання принципів доступності, зокрема низький контраст, малі

інтерактивні області, відсутність універсальних патернів для різних категорій користувачів. Виявлено неузгодженість компонентів інтерфейсу через різні стилі кнопок, карток та іконографії, неоднорідність типографіки та відсутність єдиної системи відступів. Зафіксовано високе когнітивне навантаження через надмірну кількість тексту, неінтуїтивну структуру форм та відсутність зрозумілих станів елементів.

Результати когнітивного walkthrough показали, що користувач часто стикається зі станами невизначеності, що суперечить сучасним рекомендаціям ISO 9241-110 щодо діалогових принципів інтерфейсів [4].

Редизайн виконано на основі принципів узгодженості, мінімізації когнітивного навантаження, адаптивності та доступності. Сформовано дизайн-систему, яка включає: систему відступів та модульну сітку на основі 8-point grid system; типографічну шкалу з уніфікованими стилями; кольорову палітру, що відповідає вимогам контрастності WCAG; набір UI-компонентів, включаючи кнопки, інпут-поля, навігаційні елементи, картки та діалогові вікна; дизайн-токени, які забезпечують масштабованість; патерни навігації, узгоджені з Material Design. Особливу увагу приділено мікровзаємодіям, які підсилюють передбачуваність інтерфейсу та формують відчуття плавності взаємодії [5].

Створений інтерактивний прототип моделює поведінкову логіку застосунку та демонструє ключові сценарії взаємодії. Перевірка концептуального прототипу показала покращення чіткості та послідовності навігації, читабельності та розпізнаваності основних функцій, передбачуваності переходів та логіки дій, зменшення когнітивного навантаження через структуризацію інформації.

Проведене дослідження демонструє ефективність UX-орієнтованого підходу до редизайну мобільних застосунків. Сформована дизайн-система, оптимізована інформаційна архітектура та оновлені сценарії взаємодії забезпечують підвищення доступності, узгодженості та інтуїтивності інтерфейсу. Комплексний підхід до аналізу та редизайну, що поєднує евристичну оцінку, когнітивне тестування, побудову дизайн-системи та валідацію через прототипування, дозволяє вирішити виявлені проблеми юзабіліті та підвищити якість користувацького досвіду. Перспективи подальших досліджень включають розширення дизайн-системи до повноцінної UI-бібліотеки, створення високофідельного прототипу з анімацією складних сценаріїв, проведення A/B тестування альтернативних патернів та адаптацію рішень до мультиплатформного середовища.

Список використаних джерел:

1. W3C. Web Content Accessibility Guidelines (WCAG) 2.2. URL: https://www.w3.org/TR/WCAG22/

2. Skarlatidou A., Otero C. I. Design Approaches and Human–Computer Interaction Methods to Support User Involvement in Citizen Science. *Geographic Citizen Science Design: No One Left Behind*, 2021, pp. 55–86. https://doi.org/10.2307/j.ctv15d8174.11. Accessed 16 Nov. 2025.
3. Kusuma W. A., Jantan A. H., Admodisastro N. I., & Norowi N. M. Reframed Design Thinking and Feasibility Analysis of UX Journey: Integrating User Experience and User Requirement for Solo Software Development. *Preprints*. https://doi.org/10.20944/preprints202301.0190.v1
4. ISO 9241-110:2020. Ergonomics of human-system interaction – Part 110: Interaction principles. https://www.iso.org/obp/ui/#iso:std:iso:9241:-110:ed-2:v1:en
5. Nguyen L. The Design of Everyday Things - Don Norman. https://www.academia.edu/36105941/The_Design_of_Everyday_Things_Don_Norman

Ключові слова: дизайн, UX, UI, юзабіліті, інформаційна архітектура, прототипування, доступність.
Keywords: design, UX, UI, usability, information architecture, prototyping, accessibility.

Науковий керівник: к.пед.н., доцент Лобода Ю.Г.

ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ LOW-CODE ПЛАТФОРМ ДЛЯ ПРИСКОРЕННЯ РОЗРОБКИ КОРПОРАТИВНИХ ЗАСТОСУНКІВ

Гура Володимир
доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Дацко Іван
студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Платформи із мінімальним кодуванням, так звані low-code платформи, представляють собою інноваційний підхід до розробки програмного забезпечення, що дозволяє створювати корпоративні застосунки з мінімальним обсягом написання програмного коду вручну. Такий метод розробки передбачає, що від 70 до 90% програми генерується автоматично за допомогою візуальних інструментів, зокрема переміщення елементів інтерфейсу, готових компонентів, моделей даних і бізнес-логіки.

Корпоративні застосунки являють собою програмне забезпечення, призначене для автоматизації бізнес-операцій. До них належать системи управління клієнтськими базами, фінансами, логістикою, ресурсами підприємства та робочими процесами. Традиційно розробка таких систем вимагала глибоких знань мов програмування, архітектурних шаблонів та тривалих циклів розробки, тестування і впровадження.

Платформи із мінімальним кодуванням побудовані на принципах візуального проєктування, стандартизованих програмних інтерфейсів для

обміну даними, автоматизації бізнес–процесів та гнучких методологій розробки. До найпоширеніших платформ належать Mendix, OutSystems, Microsoft Power Apps, Appian та ServiceNow App Engine. Ці інструменти дозволяють бізнес-аналітикам та громадянським розробникам створювати функціональні прототипи та повноцінні застосунки за дні або тижні замість місяців [1].

Актуальність застосування платформ із мінімальним кодуванням обумовлена декількома критичними факторами, що впливають на сучасний стан корпоративної розробки в Україні та світі.

За прогнозами аналітичної компанії Gartner, до кінця 2025 року близько 70% нових корпоративних застосунків будуть створені за допомогою технологій із мінімальним кодуванням [2]. Дослідницька компанія Forrester фіксує прискорення розробки від п'яти до десяти разів порівняно з традиційними підходами [3]. На глобальному рівні 65% організацій активно використовують такі платформи для цифрової трансформації своїх бізнес–процесів.

Ситуація в Україні характеризується гострим дефіцитом кваліфікованих розробників. За даними українського технологічного порталу DOU – найбільшої спільноти розробників України, протягом 2024 року в Україні працювало близько 80 тисяч фахівців у найбільших компаніях галузі інформаційних технологій [4]. При цьому попит на розробників значно перевищує пропозицію, особливо у сегменті досвідчених спеціалістів. Традиційна розробка корпоративних систем вимагає наявності експертів, цикл розробки триває місяці, а кошторис проектів часто перевищує бюджет.

Платформи із мінімальним кодуванням дозволяють скоротити цикл розробки до тижнів і надають бізнесу більшу самостійність у створенні внутрішніх інструментів. В Україні провідні компанії та державні установи, такі як ПриватБанк, Дія та SoftServe – українська IT компанія, що працює в сфері розробки програмного забезпечення та надання консультаційних послуг, вже активно застосовують подібні платформи для внутрішніх систем та автоматизації процесів. Потреба у швидкій цифровізації банківського сектору, державних послуг та бізнес-процесів робить ці інструменти критично важливими.

Економічна ефективність таких рішень полягає у підвищенні продуктивності розробки, скороченні списку невиконаних завдань та підтримці гнучкого підходу до управління проектами через розбиття роботи на короткі ітерації. Компанії, що не впроваджують такі рішення, ризикують відстати в цифровізації від конкурентів.

Попри численні переваги, існуючі платформи із мінімальним кодуванням мають суттєві недоліки, які обмежують їхнє повноцінне застосування в складних корпоративних середовищах.

Автоматично згенерований програмний код часто важко масштабувати в великих корпоративних системах, де потрібна інтеграція з тисячами зовнішніх сервісів або необхідно виконувати обробку мільйонів транзакцій щодня. Платформи типу Mendix чи OutSystems генерують так звану чорну скриньку коду, яку складно оптимізувати під специфічні вимоги безпеки чи продуктивності, що призводить до додаткових витрат на переробку програмного коду [5].

Дослідження показують, що в середньому 40% функціоналу корпоративних проектів все ж вимагає написання коду вручну, особливо в частинах, пов'язаних з обробкою даних у реальному часі чи дотриманням галузевих регуляцій. Це створює розрив між прототипом і остаточною версією продукту, де бізнес–користувачі стикаються з технічними труднощами.

Відсутні єдині норми для переходу з платформ із мінімальним кодуванням на повноцінні середовища розробки, що призводить до високих ризиків прив'язки до постачальника. Користувачі Mendix чи OutSystems опиняються замкненими в екосистемі постачальника, де зміна платформи може коштувати сотні тисяч доларів і місяців роботи. Платформи слабо підтримують змішані сценарії, де такі рішення поєднуються з сучасними підходами до розгортання застосунків у хмарному середовищі [6].

В Україні це особливо гостро через брак локальних постачальників і залежність від іноземних хмарних сервісів, де затримки в підтримці можуть зупинити критичні бізнес-процеси. Окремі платформи мають вузьку спеціалізацію. Наприклад, Microsoft Power Apps добре працює з інтерфейсом користувача та простими формами, але слабка в повноцінному моделюванні складних бізнес–процесів із умовними переходами та інтеграції з системами планування ресурсів підприємства. Це змушує розробників комбінувати кілька платформ, що збільшує складність та призводить до додаткових помилок на етапі інтеграції [7].

Платформи із мінімальним кодуванням часто генерують програмний код з вразливостями, які не виявляються автоматично, особливо в розширеннях, створених користувачами. Відсутність вбудованих інструментів для статичного аналізу безпеки робить їх непридатними для фінансового сектору чи державних установ, де потрібен аудит за міжнародними стандартами безпеки.

В Україні бракує шаблонів українською мовою, готових форм для державної статистики, податкової звітності чи інтеграції з Єдиним державним реєстром. Це змушує компанії витрачати тижні на ручну адаптацію базових функцій. Платформи слабо враховують специфіку роботи в умовах обмеженого доступу до глобальної мережі. Залежність від хмарних інтерфейсів може призводити до простоїв у віддалених офісах чи під час пікових навантажень. За даними Forrester, 35% проектів на таких платформах

стикаються з проблемами продуктивності при переході від прототипу до робочої версії. Прогалини в підтримці автономних режимів роблять їх менш придатними для логістики чи промисловості [3].

Для подолання виявлених обмежень та недоліків пропонується комплекс рішень удосконалення існуючих платформ із мінімальним кодуванням.

Розробка механізму експорту згенерованого коду в стандартизовані формати з можливістю подальшого редагування в середовищах розробки програмного забезпечення дозволить розробникам отримувати готові програмні модулі у вигляді контейнерів або стандартизованих конфігураційних файлів. Такий підхід передбачає впровадження стандартизованого інтерфейсу для експорту проектів, підтримку експорту бізнес-логіки в універсальних форматах та створення додатків для популярних середовищ розробки. Це знизить ризики прив'язки до постачальника на 60–70% та надасть можливість поступової міграції без повного переписування коду системи.

Вбудовування автоматизованих інструментів статичного та динамічного аналізу безпеки безпосередньо в процес розробки на платформі передбачає інтеграцію з інструментами автоматичного сканування згенерованого коду, бібліотеку попередньо перевірених та сертифікованих компонентів для фінансового сектору та державних установ, автоматичну генерацію документації з відповідності регуляторним вимогам та впровадження рольової моделі доступу на рівні платформи з аудитом усіх змін [8]. Очікується скорочення кількості критичних вразливостей на 80% та можливість проходження аудитів безпеки без додаткового переписування коду.

Створення спеціалізованого модуля для українського ринку має включати готові шаблони форм для податкової звітності, інтерфейси для інтеграції з Єдиним державним реєстром юридичних осіб, компоненти для роботи з електронним цифровим підписом згідно з українськими стандартами, шаблони документів українською мовою для різних відділів та інтеграцію з порталом Дія. Це скоротить час на адаптацію систем для українського ринку з тижнів до одного-двох днів.

Розробка проміжного програмного шару для безшовної інтеграції застосунків на платформах із мінімальним кодуванням з сучасними архітектурними підходами має включати інструменти для керування трафіком між компонентами, архітектуру, керовану подіями, для асинхронної взаємодії, підтримку функцій як розширень застосунків та автоматизовані процеси безперервної інтеграції та доставки з автоматичним тестуванням. Це дозволить використовувати платформи для 70–80% функціоналу з інтеграцією складної логіки через інші компоненти без втрати продуктивності.

Впровадження технологій прогресивних веб-застосунків та обчислень на межі мережі в застосунки на платформах із мінімальним кодуванням включає автоматичну генерацію сервісних воркерів для кешування даних та автономної роботи, синхронізацію даних через спеціальні типи даних для запобігання конфліктам при багатокористувацькому доступі, інтеграцію з платформами обчислень на межі для обробки даних ближче до користувача та оптимізацію запитів до бази даних через автоматичну генерацію індексів [9, 10]. Очікується підвищення продуктивності на 40–50% та можливість роботи у віддалених локаціях без постійного інтернет з'єднання.

Вбудована система моніторингу продуктивності застосунків та аналітики використання має включати інтеграцію з системами збору метрик у реальному часі, автоматичні рекомендації з оптимізації на основі аналізу патернів використання, проведення експериментів для компонентів інтерфейсу користувача безпосередньо в середовищі та профілювання продуктивності згенерованого коду з пропозиціями покращень. Це зменшить час на виявлення та усунення проблем продуктивності на 60% через проактивну оптимізацію до виникнення критичних ситуацій.

Запропоновані рішення та методики забезпечують комплексне усунення ключових недоліків сучасних платформ із мінімальним кодуванням та відкривають нові можливості для корпоративної розробки.

З економічної точки зору очікується зниження загальної вартості на 35–45% завдяки зменшенню ризиків прив'язки до постачальника та можливості поступової міграції. Скорочення часу виходу на ринок на 50–60% порівняно з традиційною розробкою дозволить компаніям швидше реагувати на зміни бізнес-вимог. Зменшення витрат на підтримку через автоматизований моніторинг та профілактику проблем додатково знизить операційні витрати.

Технічні переваги включають підвищення безпеки застосунків завдяки вбудованим інструментам аналізу, що критично для фінансового сектору та державних установ. Можливість створення складних систем, де платформи із мінімальним кодуванням поєднуються з іншими сучасними підходами до архітектури програмного забезпечення, розширює сферу застосування таких рішень. Покращена продуктивність та можливості масштабування через підтримку обчислень на межі мережі та оптимізацію запитів забезпечують стабільну роботу під високими навантаженнями.

Для українського ринку готові рішення для інтеграції з національними реєстрами та системами електронного урядування скоротять час впровадження. Відповідність українському законодавству у сфері захисту персональних даних, електронного цифрового підпису та податкової звітності зробить такі платформи придатними для використання в усіх секторах економіки. Скорочення часу локалізації з тижнів до днів завдяки спеціалізованому модулю дозволить компаніям швидше розпочати роботу.

Стратегічні переваги включають розширення аудиторії платформ із малого та середнього бізнесу до великих корпорацій та державних установ. Забезпечення сталого прискорення цифрової трансформації без накопичення технічного боргу дозволить компаніям підтримувати високу якість програмного забезпечення. Підвищення гнучкості інформаційної інфраструктури та зниження залежності від окремих постачальників посилить стійкість бізнесу до технологічних змін.

Соціальні переваги включають зменшення залежності від дефіциту кваліфікованих розробників через розширення можливостей для громадянських розробників. За даними DOU, у 2024 році в Україні спостерігалася найнижчий відтік фахівців із початку повномасштабного вторгнення, але дефіцит спеціалістів залишається значним. Покращення доступності державних послуг для громадян України через спрощення їх створення та підтримки посилить цифрову інклюзію. Прискорення інноваційних процесів у бізнесі та державному секторі сприятиме загальному економічному розвитку країни.

Впровадження запропонованих рішень дозволить перетворити платформи із мінімальним кодуванням з інструмента для простих задач у повноцінну альтернативу традиційній розробці для корпоративного сегмента. Це особливо актуально в умовах дефіциту фахівців в Україні та необхідності швидкої цифровізації економіки. Подальші дослідження мають зосередитися на стандартизації підходів до змішаної розробки, створенні відкритих специфікацій для сумісності між платформами та розробці галузевих бібліотек компонентів для критичних секторів економіки.

Список використаних джерел:

1. OutSystems. AI-Powered Low-Code Platform for Apps and Agents. 2024. URL: https://www.outsystems.com/low-code-platform/.
2. Gartner. Magic Quadrant for Enterprise Low–Code Application Platforms. October 16, 2024. URL: https://www.gartner.com/en/documents/magic-quadrant-for-enterprise-low-code-application-platforms.
3. Forrester Research. The Forrester Wave: Low-Code Development Platforms For Professional Developers, Q2 2023. June 20, 2023. URL: https://www.forrester.com/report/the-forrester-wave-tm-low-code-development-platforms-for-professional-developers-q2-2023/RES178497.
4. DOU. No new IT offices in Ukraine and minimal outflow of specialists since the beginning of the great war. February 17, 2025. URL: https://dev.ua/en/news/zhodnoho-novoho-it-ofisu-v-ukraini-ta-minimalnyi–vidtik–fakhivtsiv-z-pochatku-velykoi-viiny-dou-onovyv-spysok-50-naibilshykh-it-kompanii-1739779683.
5. Mendix. Mendix Named a Leader 2024 Gartner Magic Quadrant for Enterprise Low-Code Application Development Platforms For The Eighth Consecutive Year. October 21, 2024. URL: https://www.mendix.com/press/mendix-named-a-leader-2024-gartner-magic-quadrant-for-enterprise-low-code-application-development-platforms-for-the-eighth-consecutive-year/.

6. Forrester Research. The Low-Code Market Could Approach $50 Billion By 2028. March 6, 2024. URL: https://www.forrester.com/blogs/the-low-code-market-could-approach-50-billion-by-2028/.
7. Microsoft Power Platform Blog. Microsoft named a Leader in 2024 Gartner Magic Quadrant for Enterprise Low-Code Application Platforms. July 3, 2025. URL: https://www.microsoft.com/en-us/power-platform/blog/power-apps/microsoft-named-a-leader-in-2024-gartner-magic-quadrant-for-enterprise-low-code-application-latforms/.
8. Gartner. Risk and Opportunity Index: Low-Code Application Platforms. May 24, 2024. URL: https://www.gartner.com/en/documents/5459763.
9. OutSystems. Exploring low-code trends in 2024. April 12, 2024. URL: https://www.outsystems.com/blog/posts/low-code-market/.
10. Kyiv Post. Ukraine's IT Sector Experienced Lowest Staff Outflow Since Russia's Invasion. February 20, 2025. URL: https://www.kyivpost.com/post/47405.

АРХІТЕКТУРНІ ТА АЛГОРИТМІЧНІ ВИКЛИКИ КІБЕРБЕЗПЕКИ У ПРОГНОСТИЧНИХ AR-СИСТЕМАХ НА ОСНОВІ МУЛЬТИМОДАЛЬНОГО АНАЛІЗУ

Чикунов Павло

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», доцент

Пучков Владислав

аспірант Національного університету «Одеська юридична академія»

Системи доповненої реальності (AR) переживають стрімку трансформацію, переходячи від інструментів пасивної візуалізації інформації до проактивних інтелектуальних асистентів. Новітнє покоління AR-систем спрямоване на реалізацію прогностичної взаємодії – здатності системи передбачати наміри та наступні дії користувача для надання випереджувальної допомоги. Фундаментом для такої функціональності є мультимодальний аналіз поведінки, що передбачає одночасний збір, синхронізацію та інтерпретацію даних з геть різнорідних джерел: відстеження погляду (eye-tracking), аналіз жестів, розпізнавання мови, моніторинг біометричних показників (наприклад, ЕЕГ або варіабельності серцевого ритму) та просторове позиціонування [1].

Такий глибинний аналіз поведінки, хоч і відкриває значні перспективи для підвищення ефективності взаємодії «людина-машина», водночас генерує безпрецедентні виклики у сфері кібербезпеки та приватності [2]. Дані, що збираються, є не просто персональними; вони є інтимно-персональними, оскільки дозволяють робити висновки про когнітивний стан, рівень стресу, наміри та навіть стан здоров’я користувача. Компрометація таких систем може призвести не лише до витоку даних, але й до маніпуляції поведінкою користувача через нав’язування хибних прогностичних підказок.

Метою даної роботи є системний аналіз загроз кібербезпеці, притаманних архітектурі прогностичних AR-систем, та ідентифікація вразливостей на алгоритмічному рівні, пов'язаних із застосуванням моделей машинного навчання (МН) для мультимодального аналізу. Дослідження фокусується на формулюванні вимог до безпечної архітектури, що відповідає принципам «безпека та приватність за проектуванням» (Security and Privacy by Design).

Побудова життєздатної прогностичної AR-системи вимагає складної, багатошарової архітектури, кожен компонент якої має унікальні вектори атак. Типова архітектура включає такі шари.

Шар сенсорів (Sensor Layer): набір апаратних засобів (камери, мікрофони, IMU, окулографи, біосенсори), відповідальних за збір необроблених мультимодальних даних.

Шар обробки та злиття даних (Data Fusion Layer): програмний модуль, що здійснює первинну обробку, очищення, синхронізацію та злиття даних з різних джерел у єдиний вектор ознак.

Прогностичний рушій (Prognostic Engine): ядро системи, зазвичай реалізоване на базі моделей МН (наприклад, рекурентних або трансформаторних нейронних мереж), яке аналізує вектор ознак та генерує гіпотези щодо майбутніх дій користувача.

Шар візуалізації та взаємодії (Rendering & Interaction Layer): компонент, що відповідає за відображення прогностичної інформації у полі зору користувача та обробку його реакцій.

З точки зору кібербезпеки, критичні вразливості виникають на стиках цих компонентів, особливо у контексті вибору обчислювальної парадигми (on-device, edge, or cloud computing) [4].

Вразливості передачі даних. Найбільш очевидною загрозою є перехоплення необроблених сенсорних даних під час їх передачі від AR-пристрою (окулярів) до обчислювального модуля (смартфон або хмарний сервер). Потоки відео, аудіо та біометричних даних, якщо вони не захищені надійними протоколами шифрування (наприклад, TLS 1.3) та взаємною автентифікацією пристроїв, можуть бути перехоплені (атака «людина посередині»), надаючи зловмиснику повний доступ до приватної інформації користувача [6].

Безпека обчислень (On-Device vs. Cloud). Обробка даних виключно на пристрої (on-device) є найбільш бажаною з точки зору приватності, оскільки чутливі дані ніколи не залишають контрольованого користувачем середовища. Для цього використовуються високоефективні мови програмування (наприклад, C++ або Swift) та спеціалізовані бібліотеки (ARKit, ARCore, OpenCV). Однак потужність мобільних пристроїв обмежена, і складні прогностичні моделі МН часто вимагають ресурсів хмарних платформ.

Гібридна (edge-cloud) архітектура, де первинна обробка відбувається локально, а складний аналіз – у хмарі (з використанням стеку Python, TensorFlow/PyTorch), створює додаткову поверхню атаки на хмарне сховище та API, через які відбувається взаємодія [3].

Вразливості сховища даних. Мультимодальні дані та навчені моделі МН повинні безпечно зберігатися. Неналежне шифрування даних у стані спокою (at-rest) або вразливості у системі керування базами даних можуть призвести до масових витоків.

Прогностичний рушій, що є серцем системи, сам по собі є мішенню для атак, специфічних для машинного навчання.

Атаки змагальності – це клас атак, де зловмисник цілеспрямовано створює вхідні дані (наприклад, специфічний жест, візуальний артефакт або аудіошум), які є непомітними для людини, але здатні кардинально змінити висновок моделі МН [3]. В контексті прогностичної AR-системи, зловмисник може згенерувати такий «змагальний» жест, щоб змусити систему видати хибний прогноз – наприклад, приховати важливе сповіщення про небезпеку або, навпаки, ініціювати неправдиву тривогу. Це перетворює AR-систему з помічника на вектор дезінформації або маніпуляції [5].

Атаки на приватність моделі. Навіть якщо самі дані захищені, зловмисник може спробувати відновити конфіденційну інформацію, аналізуючи лише вихідні дані (прогнози) моделі. Наприклад, атаки на виведення членства (membership inference) дозволяють визначити, чи були дані конкретної людини використані під час навчання моделі. Це особливо небезпечно при аналізі медичних або поведінкових патернів.

Соціальна інженерія на основі штучного інтелекту. Комбінація мультимодального аналізу та великих мовних моделей відкриває шлях до гіперефективної соціальної інженерії. Система, що розуміє емоційний стан користувача (через аналіз голосу та міміки) та його наміри (через аналіз погляду), може бути використана для генерації надзвичайно переконливих фішингових або маніпулятивних повідомлень у реальному часі [2].

Ефективний захист прогностичних AR-систем вимагає комплексного підходу, що інтегрує безпеку на кожному етапі життєвого циклу розробки програмного забезпечення.

Принцип «Приватність за проектуванням» [4] передбачає, що механізми захисту приватності інтегруються в архітектуру системи з самого початку, а не додаються як зовнішній шар.

Це включає:

мінімізацію даних – збір лише того обсягу даних, який є абсолютно необхідним для функціонування прогнозу;

анонімізацію та псевдонімізацію – тобто усі дані, що надсилаються у хмару, мають бути позбавлені прямих ідентифікаторів;

федеративне навчання – метод навчання глобальної моделі МН на децентралізованих даних (на пристроях користувачів) без передачі самих даних на сервер;

диференційну приватність – додавання статистичного «шуму» до даних або результатів запитів до моделі, що унеможливлює точне відновлення інформації про окремого користувача, зберігаючи при цьому загальну корисність моделі.

Захист на алгоритмічному рівні. Для протидії атакам змагальності необхідно впроваджувати техніки змагального навчання, коли модель МН під час навчання цілеспрямовано «годують» змагальними прикладами, роблячи її більш стійкою до таких маніпуляцій [3]. Також необхідна розробка систем моніторингу в реальному часі, які б виявляли статистичні аномалії у вхідних даних, що можуть свідчити про спробу атаки.

Контроль з боку користувача. Ключовим аспектом, що торкається соціальних та управлінських аспектів кібербезпеки, є надання користувачеві прозорого та гранулярного контролю над тим, які мультимодальні дані збираються, коли і з якою метою.

Висновки. Прогностичні AR-системи на основі мультимодального аналізу поведінки є технологією з подвійним потенціалом: вони можуть стати потужними когнітивними помічниками або ж інструментами безпрецедентного стеження та маніпуляції. Забезпечення кібербезпеки таких систем виходить за рамки традиційного захисту мереж та даних; воно вимагає розробки нових архітектурних рішень, орієнтованих на приватність (як-от федеративне навчання), та створення нового покоління алгоритмів МН, стійких до цілеспрямованих атак. Подальші дослідження у цій галузі мають бути зосереджені на створенні комплексних фреймворків безпеки, що збалансовують високу точність прогностичної взаємодії з гарантіями конфіденційності користувача.

Список використаної літератури:

1. Popa, D., Augmented Reality and Cyber Challenges Exploration. Proceedings of the 2016 8th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2016.
2. Chen, L., On the Feasibility of Using MultiModal LLMs to Execute AR Social Engineering Attacks, 2024.
3. Ghafoor, A., Adversarial Attack Detection in AI-Based AR Systems. International Journal of Computer Science and Network Security, 25(1), pp. 120-135, 2025.
4. Roesner, F., Kohno, T., & Molnar, D. Security and Privacy for Augmented Reality Systems. Communications of the ACM (CACM), 57(4), pp. 88-96, 2014.
5. Lebeck, K. Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users. Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), pp. 53-69, 2018.

6. Al-Ghaili, M. Cybersecurity in the AI-Based Metaverse: A Survey. Applied Sciences, 2022.

Ключові слова: доповнена реальність (AR), прогностична взаємодія, мультимодальний аналіз, архітектура безпеки, кібербезпека, машинне навчання, конфіденційність даних, атаки змагальності, приватність за проектуванням.

Keywords: augmented reality (AR), predictive interaction, multimodal analysis, security architecture, cybersecurity, machine learning, data privacy, adversarial attacks, privacy by design.

АНАЛІЗ СУЧАСНИХ ІГРОВИХ РУШІЇВ GAMEDEV

Кутас Олександр

студент факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Упродовж останніх десятиліть сфера розробки відеоігор стрімко розвивається і стала одним із найдинамічніших напрямів інформаційних технологій. Важливою складовою цього процесу є створення або раціональний вибір рушія, що забезпечує технічну основу для побудови інтерактивного ігрового простору. Саме від потужності, гнучкості та оптимізації рушія значною мірою залежить якість кінцевого продукту, зручність розробки та можливість масштабування проєкту.

Раніше більшість компаній, які працювали над великобюджетними проєктами (AAA-сегментом), розробляли власні рушії, адаптовані під специфічні потреби ігор та внутрішні інструменти студій. Такий підхід забезпечував повний контроль над технічними аспектами, але вимагав значних ресурсів і часу. Натомість сучасна тенденція демонструє перехід до використання вже наявних універсальних рушіїв, як-от Unreal Engine, Unity чи Godot, які надають готові інструменти для графіки, фізики, штучного інтелекту та мережевої взаємодії. Це дозволяє розробникам зосередитися на творчій складовій ігрового процесу і не витрачати ресурси на створення базової технічної інфраструктури.

Ігровий рушій Unreal Engine має унікальні графічні можливості, які задають тенденції для всієї індустрії GameDev. Завдяки використанню низки інноваційних технологій рендерингу рушій забезпечує фотореалістичну якість зображення, яка раніше була доступна лише у високобюджетних кінематографічних середовищах. Так, технологія Nanite відповідає за віртуалізовану геометрію, що надає змогу працювати з моделями, які містять численні полігони, без втрати продуктивності [2]. Це відкриває перед розробниками нові можливості у створенні високодеталізованих світів, де навіть найдрібніші елементи залишаються чіткими та реалістичними. Система Lumen реалізує в Unreal Engine 5 глобальне освітлення та відбиття в реальному часі [1]. Вона дозволяє реалізувати максимально природне освітлення сцени без потреб тривалої попереднього оброблення або

складного налаштування джерел світла. Крім графічних переваг, рушій Unreal Engine вирізняється розвиненою архітектурою та широким набором інструментів, орієнтованих на зручність розробки. Так, система Blueprints дає змогу створювати складну ігрову логіку без глибоких знань програмування, що значно пришвидшує процес прототипування та тестування ідей [3]. Водночас рушій повністю підтримує мову C++, надаючи професіоналам можливість оптимізувати продуктивність і реалізовувати унікальні механіки. Додатково, Unreal Engine має інтегровані засоби для симуляції фізичних процесів, роботи зі звуком, анімацією та кінематографічними сценами, що робить його не просто ігровим рушієм, а повноцінним середовищем для створення інтерактивного контенту будь-якої складності. Завдяки поєднанню фотореалістичної графіки, потужних технічних інструментів і відкритої екосистеми, Unreal Engine справедливо вважається найкращим серед сучасних рушіїв для розробки ігор. Попри всі технологічні досягнення, головною проблемою залишається оптимізація. Рушій, орієнтований насамперед на фотореалістичну графіку та складні візуальні ефекти, вимагає значних апаратних ресурсів для забезпечення стабільної продуктивності. Навіть з урахуванням постійних оновлень і спроб розробників поліпшити ефективність, більшість ігор, створених на цьому рушії, залишаються доволі вибагливими до обладнання. Це особливо помітно у випадках використання новітніх технологій освітлення, відображення та геометрії, які хоч і забезпечують безпрецедентну якість візуалізації, але суттєво збільшують навантаження на систему. У результаті постає дилема між досягненням максимальної якості зображення та забезпеченням оптимальної продуктивності, що залишається одним із головних викликів для розробників, які обирають Unreal Engine як основу свого проєкту.

Рушій Unity вирізняється широкою екосистемою, підтримкою численних платформ і гнучким інтерфейсом, який дозволяє швидко створювати ітерації та тестувати ігрові механіки. Unity вирізняється низьким порогом входу, зручним інтерфейсом та широкою документаційною підтримкою, що робить його привабливим для початківців. Рушій забезпечує кросплатформенність, підтримку 2D і 3D проєктів, гнучку інтеграцію зі сторонніми інструментами (зокрема Blender і Maya), а також активну спільноту з розвиненим маркетплейсом Asset Store. Простота ітерацій, можливість розширення функціоналу та помірні апаратні вимоги сприяють ефективній розробці навіть за обмежених ресурсів. Монетизаційна модель, попри критику, залишається вигідною для інді-команд, а постійний розвиток рушія свідчить про орієнтацію на потреби користувачів [4]. Його офіційний маркетплейс Asset Store значно скорочує час розробки, оскільки дозволяє використовувати вже створені та перевірені рішення, а не будувати їх із нуля. Крім того, він формує активну спільноту розробників, які обмінюються досвідом, оновленнями та власними

напрацюваннями, що сприяє постійному розвитку екосистеми Unity. Основною проблемою даного рушія залишаються його недоліки в системі оновлень, а також зниження стабільності та рівня оптимізації під час роботи з великими проєктами.

Сильною стороною рушія Godot є його відкритість та незалежність. Він поширюється з відкритим вихідним кодом і не потребує ліцензійних платежів, що робить його безкоштовним для будь-якого типу проєктів. Це дає розробникам повну свободу у зміні рушія під власні потреби та забезпечує прозорість у роботі. Власна мова сценаріїв GDScript, подібна до Python, дозволяє швидко створювати прототипи навіть початківцям [5]. Завдяки легкості, гнучкості та активній спільноті, яка постійно вдосконалює його функціонал, Godot став популярним вибором для інді-розробників і навчальних проєктів. У випадку з цим рушієм головною проблемою є обмежені 3D-можливості. Так, порівняно з Unity, Godot наразі поступається за рівнем розвитку тривимірної графіки та фізики, що робить його менш придатним для створення високопродуктивних 3D-ігор.

Кожен із розглянутих рушіїв має свої сильні сторони та недоліки, які впливають на вибір інструменту для розробки. Unreal Engine забезпечує найвищу якість графіки та реалістичність, але водночас потребує потужного обладнання і складний в оптимізації. Unity вважається більш універсальним і зручним у використанні, проте має проблеми зі стабільністю та системою оновлень, особливо у великих проєктах. Godot, своєю чергою, приваблює відкритим кодом і простотою, але поступається конкурентам у сфері тривимірної графіки та фізики. Для проєктів невеликого масштабу або орієнтованих на легкість, оптимізацію та швидку розробку доцільним вибором є рушії Unity або Godot. Обидва ці середовища відомі своєю ефективністю, зручністю та низькими вимогами до системних ресурсів, що робить їх ідеальними для інді-проєктів, мобільних ігор або навчальних розробок.

Вибір конкретного рушія супроводжується низкою компромісів, адже кожне програмне середовище має власні переваги та обмеження. Деякі рушії показують кращу продуктивність у проєктах із високим рівнем графічної деталізації та складною фізикою, тоді як інші вирізняються простотою використання, гнучкістю або кросплатформністю. Тобто ефективність рушія безпосередньо залежить від специфіки проєкту, його масштабу, жанрових особливостей і технічних вимог команди розробників.

Отже, розвиток рушіїв у геймдеві рухається у напрямі підвищення ефективності, зручності та гнучкості. Порівняльний аналіз сучасних ігрових рушіїв GameDev – Unreal Engine, Unity та Godot – демонструє їхню диференціацію за технічними можливостями, доступністю та цільовими сегментами. Unreal Engine орієнтований на створення високореалістичних візуальних середовищ і складних механік, що робить його придатним для AAA-

проєктів, але водночас вимагає значних ресурсів. Unity забезпечує гнучкість, кросплатформність і швидке прототипування, що ідеально підходить для інді-розробки та мобільних ігор. Godot вирізняється відкритим кодом, простотою та незалежністю, проте має обмеження у 3D-графіці. Вибір рушія залежить від балансу між технічною складністю, бюджетом, масштабом проєкту та рівнем підготовки команди.

Список використаної літератури:

1. Unreal Engine 5: Lumen Global Illumination and Reflections. URL: https://dev.epicgames.com/documentation/en-us/unreal-engine/lumen-global-illumination-and-reflections-in-unreal-engine
2. Nanite Virtualized Geometry. URL: https://dev.epicgames.com/documentation/en-us/unreal-engine/nanite-virtualized-geometry-in-unreal-engine
3. Blueprints Visual Scripting. URL: https://dev.epicgames.com/documentation/en-us/unreal-engine/blueprints-visual-scripting-in-unreal-engine
4. Unity Asset Manager. URL: https://unity.com/products/asset-manager
5. Документація до Godot Engine 4.5 українською мовою. URL: https://docs.godotengine.org/uk/4.x/getting_started/introduction/introduction_to_godot.html

Ключові слова: рушій, розробка ігор, графіка, Unity, Godot, Unreal Engine.
Keywords: engine, gamedev, graphics, Unity, Godot, Unreal Engine.

Науковий керівник: к.т.н., доцент Трофименко О.Г.

СУЧАСНІ МЕТОДИ АНАЛІЗУ ДАНИХ ДЛЯ ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ

Гура Володимир

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Гандзій Ілля

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному суспільстві засоби масової інформації відіграють визначальну роль у формуванні громадської думки та соціальних процесів. Власники багатьох інформаційних каналів, керуючись інтересами бенефіціарів і спонсорів, часто подають новини під певним кутом, який може суттєво відрізнятися від реальних подій [1, 3]. Така практика призводить до спотворення фактів і поширення дезінформації, що швидко набуває вірусного характеру завдяки цифровим платформам [4]. У світі, де доступ до достовірної інформації стає стратегічним ресурсом, той, хто контролює її потік, здатен впливати на рішення людей, політичні процеси та суспільну стабільність [3, 5].

Критичне мислення, навички аналізу джерел і вміння розрізняти правду від маніпуляції стають необхідними для свідомого сприйняття процесів в інформаційному суспільстві [2,4]. Особливо гостро ця проблема проявляється в умовах цілеспрямованого впливу на окремі соціальні групи через медіа, де інтереси власників каналів часто переважають над об'єктивністю висвітлення подій і процесів у суспільстві. Як наслідок, виникає суперечливість подання новин у медійних потоках, що ускладнює сприйняття реальності та сприяє поляризації суспільства.

Активне використання комунікаційного інструменту Telegram, є наочним прикладом різноманітного інформаційного середовища. Відсутність ефективних інструментів автоматичного виявлення дезінформації в україномовному сегменті Telegram створює критичну вразливість державі, особливо в умовах гібридної інформаційної боротьби. Таким чином, розробка адаптованих технологій аналізу контенту, що розміщується в інформаційному середовищі є не лише науковим, а й суспільно-політичним пріоритетом [7].

Дослідження присвячено вивченню способів обробки медійних даних для виявлення дезінформаційного контенту у цифровому просторі. На основі аналізу наукових публікацій створено комбіновану систему, яка об'єднує текстові, візуальні, аудіо- та графові ознаки в єдине рішення. Ця система спеціально налаштована на особливості україномовного контенту в Telegram і доповнена інструментами, що пояснюють, чому саме прийнято те чи інше рішення. Перевірка на реальних даних довела кращі результати порівняно з відомими аналогами за точністю, швидкістю та зрозумілістю роботи. Новизна полягає в тому, що система враховує мовні особливості української аудиторії та робить процес перевірки прозорим для користувачів.

Сучасний інформаційний простір швидко трансформується завдяки цифровим технологіям, які впливають на те, як створюється, поширюється та сприймається контент. Великі обсяги медійних даних стають доступними всім учасникам цифрового простору, і це створює умови для широкого використання недостовірної інформації. Дезінформація – це навмисне поширення хибних відомостей з метою зміни думки чи поведінки людей. Такі дії часто поєднуються з використанням штучно створених зображень, відео чи аудіо, а також систем автоматичних акаунтів [7, 8]. Їх створення і розповсюдження може суттєво впливати на суспільну думку, виборчі процеси та інформаційну безпеку держави. Саме у цьому сенсі в українському суспільстві особливу роль відіграє комунікаційна платформа Telegram, де повідомлення поширюються дуже швидко, а контроль за її вмістом не врегульовано на законодавчому рівні. Без застосування спеціальних інструментів для перевірки це створює серйозні ризики. Тому створення систем, які працюють саме з українським сегментом контента в Telegram, є важливим завданням, як для суспільства і для держави [1].

Метою роботи є створення мультимодальної системи автоматичного виявлення дезінформації в україномовному сегменті Telegram, яка одночасно аналізує текст, зображення, аудіо/відео та мережу поширення контенту, а також містить вбудовані інструменти пояснюваності рішень. Ці інструменти забезпечують прозорість роботи системи, надаючи користувачу чітке обґрунтування кожного вердикту, які саме слова чи мовні конструкції, деталі зображення, ознаки синтезованого аудіо або аномалії в схемі поширення (наприклад, скоординована активність ботів) стали підставою для класифікації повідомлення як дезінформації, разом із кількісною оцінкою внеску кожної ознаки у фінальне рішення.

Для реалізації цієї мети проводиться огляд сучасних методів виявлення дезінформації (текстових, мультимедійних, графових та гібридних підходів), розробляється модульна архітектура системи з об'єднанням різних типів контенту (текст, зображення, аудіо/відео та мережа поширення), виконується адаптація й тонке налаштування моделей під особливості української мови, інтегруються інструменти пояснення рішень на основі оцінки внеску кожної ознаки, а також здійснюється комплексна перевірка ефективності системи на реальних прикладах україномовного контенту.

Об'єктом дослідження є інформаційні потоки контенту у Telegram, що містять текст, зображення, аудіо, інформацію про взаємодію та спосіб поширення. Предметом дослідження виступають математичні моделі, алгоритми та способи оцінки, які дозволяють автоматично визначати недостовірну інформацію з високою точністю, швидкістю та адекватністю.

Новизна роботи полягає в тому, що система вперше об'єднує аналіз кількох типів даних з урахуванням особливостей української мови та реалізує повноцінну пояснення рішень на основі оцінки внеску кожної ознаки. Це відрізняється від більшості існуючих рішень, які або не адаптовані до української мови, або працюють як «чорні скриньки» без надання зрозумілих обґрунтувань класифікації [2, 3].

Сучасні дослідження надають поступовий перехід від простих методів перевірки тексту до складних систем, що враховують кілька типів контенту одночасно. Спочатку увага зосереджувалася на словах, стилі викладання контенту, та його емоційних відтінків. Але такі способи втрачають ефективність, коли з'являлася мультимедійна складова контенту, а саме зображення чи звук. Сьогодні сучасні системи (зокрема VERA, FakesCope, Reality Defender, Meta AI Multimodal Fact-Check та Microsoft Video Authenticator) здатні одночасно аналізувати текстову, фото-, відео- та аудіоскладові контенту й виявляти невідповідності між ними, а також ознаки підробки медіафайлів.

Окремий напрямок – вивчення поширення інформаційного контенту. Дослідження демонструють, що дезінформація характеризується аномально

швидким вірусним розповсюдженням, концентрацією активності навколо обмеженої кількості ключових акаунтів та наявністю скоординованих мереж ботів і тролів [8, 11].

Це допомагає передбачити, чи стане повідомлення вірусним. Додатково аналізується поведінка акаунтів, щоб виявити ботів і фейкові/скоординовані профілі, які працюють за однаковими сценаріями та шаблонами [8].

Найперспективнішим вважається об'єднання всіх типів даних. Сучасні моделі дозволяють порівнювати текст із зображенням чи аудіо фрагментом і знаходити невідповідності [9]. Проте більшість таких рішень створено для англійської мови, тому для українського мовного сегменту потрібні спеціальні налаштування. Сучасні способи виявлення недостовірного контенту різняться за цілями, методами та інформаційними потоками, де вони розповсюджуються. Кожен спосіб має свої сильні сторони, але й обмеження, що ускладнює повне вирішення проблеми. У таблиці 1 наведено порівняльний аналіз сучасних методів виявлення дезінформації та недостовірного контенту за такими критеріями, тип даних, рівень автоматизації, підтримка української мови, швидкодія та наявність механізмів пояснення.

Таблиця 1 – Порівняння способів перевірки недостовірної інформації

Мета	**Опис**	**Канали поширення**	**Переваги**	**Недоліки**
Знайти помилки в тексті	Аналізує слова, стиль, емоції	Telegram, X, Facebook	Швидко працює з текстом	Не бачить фото чи звук
Виявити підроблені зображення	Перевіряє фото, обличчя, підписи	Instagram, TikTok, Telegram	Добре ловить deepfake	Потребує текст для порівняння
Зупинити вірусне поширення	Стежить за репостами, ланцюжками	Telegram-канали, групи	Передбачає спалах фейків	Багато обчислень
Розпізнати фальшивий звук	Аналізує голос, шум, синхронізацію з відео	YouTube, TikTok, Telegram-аудіо	Знаходить підроблені записи	Вимагає якісного аудіо
Визначити бото-мережу	Шукає шаблонні дії, частоту постів	Telegram-чати, X, ботоферми	Виявляє штучне поширення	Потребує доступу до метаданих
Перевірити метадані	Аналізує час, місце, пристрій створення	Telegram, WhatsApp, email	Доводить автентичність файлів	Не працює з видаленими даними
Виявити емоційний маніпулятив	Шукає страх, гнів, тривогу в тексті	Telegram-канали, соцмережі	Блокує психологічний тиск	Складно відрізнити від емоцій
Повне виявлення фейків	Об'єднує текст, фото, звук, мережу	Усі платформи (Telegram, X, Meta)	Найточніший результат	Потребує налаштуванн я під мову

Важливим стало питання пояснення прийнятих рішень – тобто чому система класифікувала конкретне повідомлення саме як дезінформацію. Системи аналізу контенту повинні не просто визначити недостовірну інформацію, а довести, чому саме вона класифікована, як недостовірна. Для цього використовують методи, які вказують, які частини контенту найбільше вплинули на визначення їх класифікації.

Для аналізу використано набір реального контенту з платформ Telegram, X та Meta (текст, зображення, аудіо та відео), доповнений спеціально зібраною україномовною базою текстових, візуальних і мультимедійних матеріалів. Увесь контент пройшов ретельну анонімізацію та видалення персональних метаданих для забезпечення конфіденційності джерел.

Спочатку контент звільнюється від метаданих та розбивається на частини. Текстова складова обробляється спеціальною моделлю для української мови, аудіо- та відеофрагменти обробляються моделями розпізнавання та верифікації (Whisper + спеціалізовані детектори deepfake-аудіо), що порівнює картинки з текстом. Мережа поширення аналізується за швидкістю розповсюдження та зв'язками між акаунтами. Усі зроблені класифікації зводяться разом, і система вирішує, чи є контент достовірним.

Після класифікації система чітко пояснює своє рішення та показує користувачу, які саме слова, деталі фото, фрагменти аудіо чи аномалії поширення «переважили» і чому повідомлення визнано дезінформацією. Пояснення формується за допомогою стандартних методів інтерпретації, які кількісно оцінюють внесок кожної ознаки у кінцевий результат [5].

Система побудована за принципом поетапної обробки. Спочатку контент надходить у кілька паралельних блоків, один відповідає за текст, другий за зображення, третій за аудіо складову, четвертий за мережу поширення. Кожен блок видає свій класифікатор, а потім усі результати об'єднуються з урахуванням того, наскільки важлива кожна складова у кожному контенті.

Для ефективного виявлення недостовірного контенту використовується комбінація традиційних і сучасних інструментів [3, 5, 9]. Кожен з них має свою сферу застосування, але разом вони створюють надійну основу для аналізу. Перевірка фактів, аналіз джерел і змісту, моніторинг соцмереж та залучення експертів – це перевірені методи, які доповнюють автоматизовану класифікацію контента. Їхня адаптація до україномовного сегменту платформи Telegram вимагає урахування локальних особливостей, мовних нюансів, культурного контексту та лексичної специфіки. Порівняння цих інструментів наведено в таблиці 2.

Таблиця 2 – Інструменти виявлення недостовірних новин

Інструмент	Опис	Як працює на практиці	Переваги	Недоліки	Адаптація до української мови
Перевірка фактів	Перевірка правдивості фактів у новинах через аналіз джерел, пошук доказів та порівняння з надійними базами	Журналісти чи аналітики беруть заяву, шукають першоджерело, перевіряють документи, фото, свідчення	Висока точність при наявності доказів	Потребує часу та доступу до джерел	Потрібні відкриті бази перевірених фактів українською
Дослідження джерел	Оцінка надійності видання: репутація, акредитація, історія, авторство	Перевіряється, хто написав, хто володіє каналом, чи є ліцензія, чи є спростування в минулому	Допомагає відсікати сумнівні канали	Не завжди є публічна інформація	Адаптація через реєстр українських ЗМІ та Telegram-каналів
Аналіз змісту	Вивчення тексту, фото, відео на логіку, послідовність, підробки	Шукають невідповідності: старе фото в новій події, нелогічні аргументи, підроблені цитати	Виявляє маніпуляції в деталях	Складно з сарказмом чи гумором	Потребує україномовних моделей для аналізу стилю
Моніторинг соцмереж	Відстеження поширення, трендів, активності акаунтів	Аналіз репостів, реакцій, хто і як швидко ділиться	Передбачає вірусність фейків	Багато шуму, потрібні фільтри	Фокус на Telegram-каналах і групах
Експертні оцінки	Залучення фахівців для аналізу теми	Експерт оцінює за своїм досвідом: лікар — медичні фейки, історик — історичні	Глибоке розуміння теми	Суб'єктивність, час	Потрібні українські експерти з різних галузей

Як видно з таблиці 2, жоден інструмент не є універсальним і вони доповнюють один одного. У пропонованій системі ці методи інтегровано в автоматизовану платформу, перевірка достовірності фактів – через аналіз джерел і змісту, моніторинг – через граф поширення, тобто схему зв'язків між акаунтами, де видно, хто, коли і як швидко поширює повідомлення (репости, коментарі та їх ланцюжки), експертні оцінки – через пояснення, тобто автоматичне визначення, які саме слова, деталі зображення чи зв'язки

найбільше вплинули на рішення системи, ніби «експерт» пояснює свої висновки. Адаптація до української мови досягається за допомогою спеціалізованих моделей, таких як ukrBERT – це українська версія моделі BERT (Bidirectional Encoder Representations from Transformers), яка є одним із найпоширеніших інструментів для обробки природної мови [8]. Модель навчається на великому наборі україномовних текстів, включаючи новини, Вікіпедію, соціальні мережі та літературу – загалом понад 100 мільйонів слів та їх комбінацій. UkrBERT вміє розуміти контекст речень, розпізнавати емоції, стиль письма та маніпулятивні конструкції, такі як перебільшення чи приховані упередження [7, 11, 15]. Наприклад, якщо в повідомленні є фраза з емоційним забарвленням, як "шокуюча правда про вакцини", модель може виявити, що це не відповідає існуючим фактам, базуючись на набутих шаблонах україномовного підробленого медіаконтенту. Адаптація до української мови робить її ефективною для платформи Telegram, де змішується літературна мова та її діалекти, підвищуючи точність на 5–10% порівняно з загальними моделями [1, 2]. Доступна на платформі Hugging Face (відкритий репозиторій моделей машинного навчання) для подальшої адаптації та інтеграції під конкретні завдання, як дезінформація, та UkrCLIP – це українська адаптація моделі CLIP (Contrastive Language-Image Pretraining), розроблена для зв’язку тексту та зображень. Вона навчається на парах "текст-зображення" з україномовних джерел, таких як новина з фото чи пости в Instagram, – понад 100 тисяч прикладів. Модель перевіряє, чи відповідає зображення опису в тексті: наприклад, якщо новина про "протести в місті" містить фото з міста іншої країни, UkrCLIP виявить невідповідність [14]. Вона також розпізнає підробки зображень, такі як підроблений медіаконтент, за абстрактами пікселів і стилем. Адаптація до української мови враховує локальні візуальні шаблони, як українські прапори чи символи, що робить її корисною для перевірки контенту в Telegram. Точність зростає на 7–12 % для україномовних пар текст-зображення порівняно з базовою CLIP, яка орієнтована на англійську [3, 4]. Модель доступна на GitHub і Hugging Face для інтеграції в системи перевірки достовірності фактів.

Ці моделі роблять систему гнучкою для україномовного сегменту, де недостовірна інформація часто опановує певні теми. Навчання на контенті з українських джерел, таких як UA-News чи UA-Wiki, дозволяє уникнути помилок через переклад. Наприклад, ukrBERT може розпізнати маніпуляцію в фразі "секретна правда про подію", а UkrCLIP – перевірити супровідне фото. Загалом, така адаптація підвищує загальну ефективність системи на 10–15%, роблячи її придатною для реального використання в Telegram [5, 7]. Це дозволяє системі працювати швидше та точніше, ніж ручні методи. Такий підхід робить процес перевірки контенту прозорим і доступним для широкого кола користувачів. UkrCLIP, які навчені на україномовному контенті. Ці моделі

дозволяють системі точно аналізувати текст і зображення, враховуючи особливості української мови, такі як морфологія, синтаксис і культурний контекст. Без такої адаптації моделі, створені для англійської чи інших мов, часто помиляються через відмінності у словнику, граматиці чи ідіомах, що знижує точність виявлення недостовірного контенту [10, 11, 16].

Запропонована система для виявлення дезінформації в україномовному сегменті Telegram побудована за модульним принципом. Вона складається з кількох блоків, які працюють одночасно, що дозволяє швидко обробляти великий потік даних і давати точний результат.

На вході система приймає контент з Telegram, а саме текстові повідомлення, зображення, аудіо-, відео-, а також інформацію про те, хто і коли його опублікував, як його поширюють – через репости, коментарі чи реакції.

Перший блок відповідає за аналіз текстового контенту. Він перевіряє, чи є в повідомленні маніпуляції, перебільшення, емоційне забарвлення, відсутність джерел або логічні невідповідності. Для цього використовується спеціальна модель, навчена на україномовних текстах.

Другий блок аналізує зображення. Він порівнює, чи відповідає зображення опису в тексті. Наприклад, якщо повідомлення говорить про одну подію, а фото – з іншої, система це помітить. Також перевіряються ознаки підробки зображень.

Третій блок аналізує аудіо. Він розпізнає мову, визначає, чи є голос справжнім, чи синтезованим, і перевіряє, чи збігається звук із рухами губ у відео.

Четвертий блок стежить за поширенням. Він дивиться, як швидко і ким поширюється повідомлення, чи є шаблонні дії, що вказують на ботоферми або скоординовану кампанію.

Усі висновки з чотирьох блоків збираються в одному місці. Система автоматично визначає, наскільки важлива кожна частина даних у конкретному випадку – наприклад, якщо немає аудіо, його вплив не враховується.

Далі працює блок пояснення, він показує, які саме слова, деталі зображення чи зв’язки між акаунтами вплинули на рішення. Це робить процес прозорим – аналітик бачить, чому система вважає повідомлення підозрілим.

На останньому етапі система приймає рішення, це правда чи фейк. Результат виводиться на зручний інтерфейс перегляду – з графіками, прикладами, поясненнями та можливістю експорту даних.

Система працює швидко, адаптована до української мови і може бути встановлена навіть на простих пристроях. Вона перевершує окремі текстові чи візуальні моделі, бо враховує всі типи даних і пояснює свої дії.

Робота системи перевіряється за кількома показниками, наскільки точно вона знаходить недостовірну інформацію, як швидко реагує та наскільки зрозуміло пояснює свої дії. Усе це об'єднується в одну оцінку.

Система була протестована на наборі з реальних повідомлень з платформи Telegram. Дані включали текст, зображення, аудіо, відео та метадані про поширення – усе очищене від особистих відомостей. Тестування проводилося в режимі імітації живої роботи, повідомлення надходили по одному, як у реальному часі, з випадковими інтервалами від 1 до 30 секунд. Систему було реалізовано на звичайному сервері без спеціалізованого обладнання. Кожне повідомлення оброблялося повністю, від аналізу тексту до присвоєння класифікації та пояснення.

Порівняння проводилося з трьома відомими рішеннями – ukrBERT (тільки текст), UkrCLIP (текст + зображення) та Whisper + GraphSAGE (аудіо + поширення). Усі моделі тестувалися за однакових умов, той самий набір даних, той самий сервер, той самий порядок повідомлень. Жодна модель не мала доступу до додаткових ресурсів чи попередньої інформації.

Результати показали, що розроблена система перевершує аналоги за всіма трьома критеріями, точністю, швидкістю та зрозумілістю. Вона досягла балансa між точністю та повнотою моделі класифікації 0,94, тоді як ukrBERT – 0,89, UkrCLIP – 0,91. Час реакції склав менш 3 секунд на повідомлення, що лише на 0,5 секунди повільніше за найшвидший окремий блок, але з повним поясненням.

Тестування показало, що об'єднання в одній системі всіх типів даних (текст + зображення + аудіо + граф поширення) дає суттєво кращий результат, ніж окремі моделі. Перевірка в реальних умовах (імітація живого потоку з Telegram) підтвердила готовність системи до розгортання.

В результати створено комбіновану систему для перевірки недостовірного контенту в Telegram з урахуванням особливостей української мови. Вона об'єднує різні типи контенту, швидко реагує та пояснює свої дії. Перевірка на реальних прикладах довела її перевагу.

Список використаних джерел

1. Alenezi F. From Misinformation to Insight: A Systematic Review of AI-Driven Solutions for Combating Fake News. Information, 2025, vol. 16, no. 3, p. 189. DOI: 10.3390/info16030189. PDF: https://www.mdpi.com/2078-2489/16/3/189/pdf.
2. Almarashy H., et al. Artificial Intelligence in the Battle Against Disinformation and Misinformation: A Systematic Review of Challenges and Approaches. Journal of Artificial Intelligence and Capsule Networks, 2025, vol. 7, no. 1, pp. 69–90. DOI: 10.36548/jain.2025.1.006. PDF: https://www.researchgate.net/publication/388421309.
3. Buchanan, J., et al. Fake News, Disinformation and Misinformation in Social Media: A Review. Social Network Analysis and Mining, 2023, vol. 13, no. 1, p. 69. DOI:

10.1007/s13278-023-01028-1. PDF: https://link.springer.com/content/pdf/10.1007/s13278-023-01028-1.pdf.
4. Choras M., et al. Machine Learning and Deep Learning Applications in Disinformation Detection: A Bibliometric Assessment. Electronics, 2024, vol. 13, no. 22, p. 4352. DOI: 10.3390/electronics13224352. PDF: https://www.mdpi.com/2079-9292/13/22/4352/pdf.
5. De Fraga T., et al. AI in Disinformation Detection: A Review of Techniques and Challenges. ACIG Journal of Computer Science, 2024, vol. 2, no. 1, pp. 1–20. DOI: 10.47861/acigs.2024.2.1.1. PDF: https://www.acigjournal.com/AI-in-Disinformation-Detection,200200,0,2.html.
6. X. Men, V. Y. Mariano, "Explainable Fake News Detection Based on BERT and SHAP Applied to COVID-19", International Journal of Modern Education and Computer Science, Vol.16, No.1, pp. 11-22, 2024.
7. Choras, M., et al. Machine Learning and Deep Learning Applications in Disinformation Detection. Electronics, 2024, vol. 13, no. 22, p. 4352. URL: https://www.mdpi.com/2079-9292/13/22/4352.
9. Freeze, M., Baumgartner, M., et al. Fake news, fast and slow: Deliberation reduces belief in false (but not true) news headlines. Journal of Experimental Psychology: General, 2020, vol. 149, no. 8, pp. 1608–1613. URL: https://doi.org/10.1037/xge0000729.
10. Schnellenbach, J. The economics of fake news. CESifo Economic Studies, 2020, vol. 66, no. 3, pp. 207–227. URL: https://doi.org/10.1093/cesifo/ifaa011.
We Are Social & Hootsuite.Digital 2025: Global Report. 2025. URL: https://datareportal.com/reports/digital-2025-global-overview-report.
11. Alenezi, F. From Misinformation to Insight: A Systematic Review of AI-Driven Solutions for Combating Fake News. Information, 2025, vol. 16, no. 3, p. 189. URL: https://www.mdpi.com/2078-2489/16/3/189.
12. Kaliyar R., Goswami A., Narang P. (2021). DeepFakE: improving fake news detection using tensor decomposition-based deep neural network. The Journal of Supercomputing. V. 77. P. 1015-1037. https://doi.org/10.1007/s11227-020-03294-y.
13. Martel C., Pennycook G., Rand D. (2020). Reliance on emotion promotes belief in fake news. Cognitive Research: Principles and Implications. V. 5 (1). P. 47. https://doi.org/10.1186/s41235-020-00252-3.
14. Palani B., Elango S., Viswanathan V. (2022). A multimodal deep learning framework for automatic fake news detection using capsule neural network and BERT. Multimedia Tools and Applications. V. 81. P. 5587-5620.
15. Pehlivanoglu D., Lin T. et al. (2021). The role of analytical reasoning and source credibility on the evaluation of real and fake full-length news articles. Cognitive Research: Principles and Implications. V. 6: 24. https://doi.org/10.1186/s41235-021-00292-3.
16. Verstraete M., Bambauer D.E., and Bambauer J.R. (2017). Identifying and Countering Fake News. Arizona Legal Studies Discussion Paper. V. 73 (3). Available at: https://repository.uchastings.edu/hastings_law_journal/vol73/iss3/6.

РОЗРОБКА ОСВІТНЬОГО МОДУЛЯ «РЕФАКТОРИНГ ЗАДАЧ УЗАГАЛЬНЕННЯ ОБЄ'КТІВ»

Чикунов Павло

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», доцент

Колеснік Євгеній

магістрант Бахмутського навчально-наукового професійно-педагогічного інституту Харківського національного університету імені В. Н. Каразіна

Стрімкий розвиток штучного інтелекту, інтенсивне використання машинного навчання та нейромереж у прикладному програмуванні актуалізують проблему якості програмного коду. У сучасних умовах, коли розроблення складних систем здійснюється багатьма командами одночасно, дедалі частіше виникає явище так званого «spaghetti code» або «брудного коду» – коду з хаотичною структурою, низькою читабельністю та відсутністю архітектурної логіки. Подолання цієї проблеми можливе через систематичне застосування рефакторингу – процесу поліпшення структури коду без зміни його зовнішньої поведінки [1].

Сучасна професійна підготовка фахівців у галузі цифрових технологій вимагає не лише володіння мовами програмування, а й розуміння принципів побудови якісного, масштабованого та підтримуваного коду. Навчання рефакторингу мовою C# сприяє розвитку у студентів системного мислення, розуміння архітектури програмних систем і принципів SOLID.

Аналіз освітніх програм українських і закордонних університетів показав, що тематика рефакторингу здебільшого розглядається лише у контексті принципів SOLID або архітектурних патернів, проте не як окремий навчальний компонент.

Для підвищення ефективності підготовки запропоновано створення освітнього модуля, присвяченого групі прийомів «Dealing with Generalization (задачі узагальнення об'єктів)» за класифікацією Мартіна Фаулера [2].

Модуль складається з трьох лабораторних робіт:

1. підйом і спуск елементів у ієрархії класів – прийоми Pull Up Field, Pull Up Method, Push Down Field, Push Down Method;

2. побудова та оптимізація ієрархії класів – прийоми Extract Subclass, Extract Superclass, Extract Interface, Collapse Hierarchy;

3. Узагальнення поведінки та трансформація механізмів наслідування – прийоми Form Template Method, Pull Up Constructor Body, Replace Inheritance with Delegation, Replace Delegation with Inheritance.

Виконання лабораторних робіт передбачає аналіз «брудного коду», розроблення «чистих» рішень із застосуванням принципів інкапсуляції,

поліморфізму та повторного використання коду, побудову UML-діаграм ієрархій класів та функціональне тестування у IDE Visual Studio. Це сприяє розвитку у студентів компетентностей високого рівня – аналітичного, архітектурного та методичного мислення [3].

Лабораторні роботи реалізує діяльнісний та компетентнісний підходи до професійної підготовки майбутніх викладачів цифрових технологій. Її структура побудована за принципом “від теорії до практики” – спочатку здобувач опрацьовує теоретичний матеріал щодо сутності групи прийомів «Задачі узагальнення об’єктів», після чого переходить до поетапного їх застосування.

Усі три лабораторні роботи, що входять до освітнього модуля «Рефакторинг задач узагальнення об’єктів», мають єдину методичну структуру, яка забезпечує цілісність навчального процесу та поступове формування професійних компетентностей здобувачів освіти.

Кожна робота включає п’ять основних етапів:

– опрацювання теоретичних положень щодо групи прийомів рефакторингу;

– проєктування предметної області за індивідуальним варіантом;

– виконання рефакторингу «брудного коду» з використанням прийомів;

– побудову UML-діаграм до та після змін;

– підготовку звіту із коментарями та порівняльним аналізом результатів.

Методологічно робота поєднує елементи проектного навчання (створення власної предметної області у вигляді міні-проєкту) та проблемного навчання (усунення «брудного коду» шляхом рефакторингу).

Завдання побудовані так, щоб забезпечити послідовний розвиток умінь від аналізу коду до його вдосконалення із використанням прийомів рефакторингу.

Особлива увага приділяється самостійному виявленню проблем архітектури, побудові UML-діаграм і документуванню змін, що сприяє розвитку у студентів критичного мислення, навичок технічного письма та розуміння архітектурної чистоти програмного продукту.

Таким чином, лабораторна робота виконує не лише навчальну функцію, але й методичну – формуючи в майбутніх фахівцях готовність навчати інших рефакторингу як інструменту підвищення якості програмних систем.

Подальший напрямок передбачає не лише вдосконалення змісту освітнього модуля, а й розширення його функціональності у напрямі інтелектуалізації освітнього процесу, що сприятиме підготовці фахівців нового покоління – здатних ефективно працювати в умовах штучного інтелекту, цифрової трансформації та швидких змін технологічного середовища.

Список використаної літератури:

1. Robert C. Martin. Clean Code: A Handbook of Agile Software Craftsmanship. Prentice Hall, 2008.
2. Fowler, M. Refactoring: Improving the Design of Existing Code. 2nd Edition. Addison-Wesley, 2018.
3. Швець О. Гуру рефакторингу: український переклад прийомів Мартіна Фаулера. – URL: https://refactoring.guru/uk/refactoring

Ключові слова: освітній модуль, рефакторинг, задачі узагальнення об'єктів, лабораторні роботи.
Keywords: educational module, refactoring, dealing with generalization, laboratory works.

ПЕРСПЕКТИВИ СТВОРЕННЯ КЛАСТЕРУ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Горбаченко Станіслав

завідувач кафедри кібербезпеки Національного університету «Одеська юридична академія», доктор економічних наук, професор

Саврацький Олександр

аспірант кафедри кібербезпеки Національного університету «Одеська юридична академія»

Кібербезпека залишається одним із ключових пріоритетів національної безпеки України в умовах триваючої гібридної агресії російської федерації, яка супроводжується масованими кібератаками на критичну інфраструктуру, державні органи та приватний сектор. Згідно зі Стратегією кібербезпеки України, затвердженою Указом Президента № 447/2021 від 26 серпня 2021 року, розвиток безпечного кіберпростору передбачає посилення координації між державою, бізнесом, академічною спільнотою та міжнародними партнерами на принципах стримування, стійкості та взаємодії [1].

Національний кластер кібербезпеки (National Cybersecurity Cluster) був створений у 2021 році Національним координаційним центром кібербезпеки при РНБО України за підтримки Фонду цивільних досліджень та розвитку США (CRDF Global) та Державного департаменту США. Ця платформа об'єднує державні органи, приватні компанії, міжнародних партнерів (НАТО, ЄС, США) та експертну спільноту [2]. Станом на 2025 рік проведено понад 35 сесій кластера, включно з регіональними (Чернівці, Вінниця, Львів) та міжнародними заходами за участю Tallinn Mechanism.

Ринок кібербезпеки України демонструє стійке зростання: за оцінками DataDriven Research&Consulting, у 2024 році його обсяг сягнув 138 млн дол. США (у 4 рази більше, ніж у 2016-му), а прогноз на 2025–2029 роки — середньорічне зростання 8,54 % до приблизно 209 млн дол. США у 2029 році [3]. Війна стала потужним каталізатором розвитку вітчизняних продуктів та залучення грантів від USAID, ЄС і НАТО.

Розвиток кластерної моделі відкриває низку стратегічних перспектив. Інституційне посилення передбачає створення регіональних хабів та глибшу інтеграцію з центрами компетенцій НАТО (зокрема, Cooperative Cyber Defence Centre of Excellence у Таллінні). У 2025–2026 роках планується розширення співпраці з Румунією, Молдовою та країнами Західних Балкан [2].

Значну роль відіграватиме кадровий напрям: реформа підготовки фахівців, програми перепідготовки ветеранів (за підтримки США та Австралії), розвиток сертифікаційних центрів при Держспецзв'язку [4] та співпраця з Neoversity. Це дозволить частково закрити дефіцит спеціалістів, який на кінець 2025 року оцінюється у 25-30 тис. осіб.

Інноваційний та економічний потенціал кластера полягає у прискореній комерціалізації рішень на базі ШІ, захисту мереж, blockchain та постквантової криптографії. Завдяки координації через кластер Україна вже експортує окремі продукти до країн Азії та Європи, а до 2030 року сектор може стати одним із драйверів економічного відновлення [5].

Міжнародна інтеграція відкриває доступ до фінансування (програми USAID «Кібербезпека критичної інфраструктури України», гармонізація з директивою NIS2 ЄС) та обмін досвідом. Україна демонструє унікальну стійкість та попри зростання атак на 70% у 2024, ринок також розширюється. Дослідження DataDriven, ініційоване EBA та Асоціацією IT України, показує, що ринок кібербезпеки України досяг 138 мільйонів доларів, що в чотири рази більше, ніж у 2016 році. Прогнозується, що до 2029 року він зросте ще на 50% і перевищить 200 мільйонів доларів [6].

Попри виклики (недостатнє бюджетне фінансування — близько 0,15 % від видатків держбюджету проти 1-4 % у розвинених країнах, залежність від імпортного обладнання), кластерна модель вже довела свою ефективність і продовжує еволюціонувати в повноцінну національну екосистему кібербезпеки. Подальше розширення до спеціалізованих підкластерів (фінансовий сектор, енергетика, біокібербезпека) та посилення державно-приватного партнерства дозволить Україні не лише надійно захищатися, а й стати регіональним експортером кібертехнологій у Європі.

Список використаних джерел:

1. Указ Президента України № 447/2021 «Про рішення Ради національної безпеки і оборони України від 27 серпня 2021 року «Про Стратегію кібербезпеки України»». Офіційне інтернет-представництво президента України. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 18.11.2025).
2. Національний кластер кібербезпеки. Офіційний сайт. URL: https://cybersecuritycluster.org.ua (дата звернення: 18.11.2025).
3. Фещенко Ю. Український ринок кібербезпеки оцінили в $138 млн. Як він змінився та чого від нього чекати. MC.today. URL: https://mc.today/uk/ukrayinskij-rinok-kiberbezpeki-otsinili-v-138-mln-yak-vin-zminivsya-ta-chogo-vid-nogo-chekati/ (дата звернення: 18.11.2025).
4. Держспецзв'язку та eGA запускають проєкт з підвищення кіберстійкості критичної інфраструктури. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/ssscip-and-ega-to-enhance-cyber-resilience-of-ukrainian-critical-infrastructure (дата звернення: 19.11.2025).

5. Ukraine's tech market: 2025 report. N-ix. URL: https://src.n-ix.com/uploads/2025/02/25/d3f17988-8246-40ae-9703-3cd14f6163ad.pdf (дата звернення: 19.11.2025).
6. Ukraine's Cybersecurity Market to Hit $200M as Attacks Grow in Sophistication. IT Ukraine Assosiation. URL: https://itukraine.org.ua/en/ukraine-s-cybersecurity-market-to-hit-200m-as-attacks-grow-in-sophistication/ (дата звернення: 19.11.2025).

Ключові слова: кібербезпека, кластер кібербезпеки, кіберстійкість, кібератаки, критична інфраструктура.
Keywords: cybersecurity, cybersecurity cluster, cyber resilience, cyberattacks, critical infrastructure.

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ТОКСИЧНОГО КОНТЕНТУ ПРИ СПІЛКУВАННІ УКРАЇНСЬКОЮ МОВОЮ

Гура Володимир
доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Касян Павло
студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасний етап розвитку цифрових платформ висуває нові вимоги до модерації контенту в українських онлайн-спільнотах. За даними дослідження, опублікованого у 2025 році, 68% користувачів стикаються з токсичними повідомленнями щотижня, а 42% припиняють активність у спільнотах через психологічний тиск [1]. Найбільш гостро ця проблема проявляється у групових чатах месенджерів і соціальних мереж, де відсутність професійних модераторів поєднується з постійним збільшенням токсичного контенту. Саме ці фактори стали основним стимулом для розробки автоматизованої системи аналізу та виявлення прямих образ, сарказму, мікроагресії та групового тиску в реальному часі.

Аналіз методів виявлення токсичного контенту проведено на основі огляду наукових джерел за період 2023 – 2025 років. Аналіз охопив лексичні, семантичні, графові, контекстні та гібридні підходи, з акцентом на підтримку української мови у контексті виявлення прихованої агресії. Як встановлено у дослідженні, лише 12 % інструментів підтримують мови з низьким рівнем ресурсів, до яких належить українська, а 79% систем фокусуються виключно на прямих образах, ігноруючи імпліцитну агресію [2]. Більшість рішень не адаптовано до української мови і потребують значних обчислювальних ресурсів або зовнішніх сервісів. Крім того, приховані форми токсичності, такі як сарказм, невербальні маркери та контекст, залишаються поза увагою.

Дослідження на конференції NAACL 2025 показало, що 74% токсичних діалогів містять невербальні індикатори, наприклад, глузливі емодзі [3].

Лексичні методи, представлені в дослідженнях CEUR-WS 2025 та WOAH 2024, базуються на словниках заборонених слів і досягають точності до 70 % при виявленні прямих образ, але ігнорують сарказм і мікроагресію [4, 9]. Семантичні підходи на основі BERT-моделей (Bidirectional Encoder Representations from Transformers) працюють інакше. BERT – це нейронна мережа, яка навчається на величезних текстах і «розуміє» слова в контексті з обох боків. Наприклад, слово «банк» вона розрізняє як фінансову установу або берег річки залежно від сусідніх слів. Для токсичності BERT навчають на мільйонах прикладів, де позначено токсичні та нетоксичні тексти. Після навчання модель може передбачати, чи фраза образлива, навіть якщо в ній немає грубих слів. Але для хорошої роботи потрібні дуже великі набори текстів (мільйони прикладів) і потужні відеокарти, бо навчання займає дні або тижні. Для української мови це проблема, бо готових текстових наборів даних мало, тому моделі часто «до навчають» на перекладених даних з англійської [5]. Графові методи, використовують аналіз структури діалогу для виявлення групового тиску, досягаючи 78 % повноти при фіксації атак чотирьох і більше учасників [11]. Контекстні моделі враховують попередні репліки, додаючи 12% до виявлення сарказму [6].

Гібридні підходи, такі як у BIS 2025, поєднують BERT з правилами та досягають 89 % точності, але залежать від інтернету та хмарних сервісів [8]. Жоден з проаналізованих методів не забезпечує одночасно автономність, підтримку української мови, виявлення всіх форм токсичності та пояснення результатів. Це підтверджує необхідність нової системи, яка усуває ці недоліки.

Для подолання цих недоліків розроблено гібридний алгоритм ToxDialHybrid – автономну, ефективну та точну систему модерації діалогів українською мовою. Алгоритм базується на послідовному багатошаровому аналізі з використанням п’яти взаємодоповнюючих методів, які охоплюють як явні, так і приховані форми токсичності. Реалізація виконана на мові Python з бібліотекою NetworkX, що дозволяє будувати спрямовані графи, обчислювати групу метрик, які показують, наскільки той чи інший вузол є «важливим» або «центральним» у мережі, виявляти кластери та аномалії в структурі діалогу, такі як сплески семантичної активності навколо одного учасника. Анонімізовані результати зберігаються локально в базі даних SQLite без передачі даних.

Гібридний алгоритм складається з п’яти модулів, що працюють у визначеній послідовності. Спочатку активується модуль лексичного аналізу, який швидко сканує текст на наявність заборонених слів зі словника (понад 1200 елементів, включаючи ненормативну лексику та дискримінаційні

терміни). Далі модуль аналізу тональності виявляє сарказм через контраст позитивних і негативних елементів, наприклад, поєднання слова «чудово» з емодзі «невдоволене обличчя». Він використовує правила на основі структурованих колекцій текстів українською мовою [4]. Наступним є модуль графового аналізу, який будує мережу діалогу, рахує вхідні повідомлення та застосовує алгоритм PageRank – метод оцінки важливості учасників, що моделює випадковий перехід за відповідями. Якщо один користувач отримує чотири і більше відповідей від різних джерел за короткий час, фіксується груповий тиск. PageRank враховує не тільки кількість, а й якість зв'язків: відповіді від активних учасників підвищують ранг. Наприклад, повторювані повідомлення від одного джерела менш значущі, ніж розподілені від кількох. PageRank підвищує точність виявлення тиску на 14% порівняно з простим підрахунком [14]. Потім модуль невербальних маркерів аналізує емодзі, лапки, повторення – глузливий смайл додає бал токсичності. Завершальний модуль контекстного аналізу враховує до трьох попередніх реплік для виявлення зміни тону, наприклад, від нейтрального до агресивного.

Кожен модуль видає оцінку від 0 до 1, яка зважується та підсумовується за формулою 1, де S – загальний бал токсичності (остаточна оцінка повідомлення), L – лексичний аналіз (прямі образи, лайка, заборонені слова), T – аналіз тональності (сарказм, іронія через контраст (позитив + негативний маркер)), G – графовий аналіз (груповий тиск, скоординовані атаки), N – невербальні маркери (емодзі, лапки, повторення) C – контекстний аналіз (зміна тону в попередніх репліках).

$$S = 0{,}15L + 0{,}35T + 0{,}20G + 0{,}15N + 0{,}15C \qquad (1)$$

При $S > 0{,}6S$ повідомлення класифікується як токсичне. Система надає пояснення, наприклад, «Токсично через сарказм ($T = 0{,}9$) + груповий тиск ($G = 0{,}8$)». Внесок модулів у загальний бал токсичності зображено на рисунку 1.

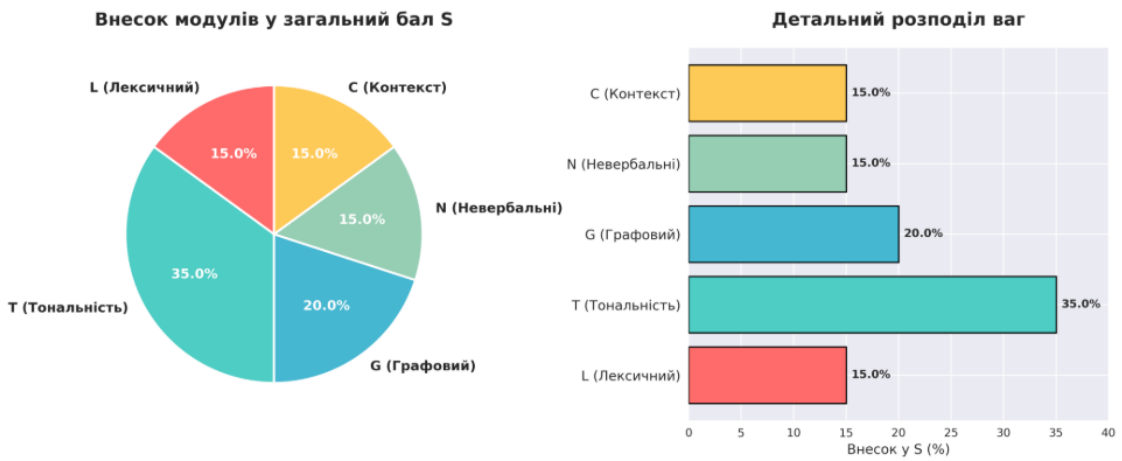

Рис. 1. Внесок модулів у загальний бал токсичності S

Ваги визначено через збір даних для перевірки та отримання висновків – тобто на основі реальних експериментів і аналізів на тестових наборах даних з більш ніж 10000 анотованих діалогів, зібраних з відкритих джерел.

Такий підхід означає, що ваги підбиралися шляхом багаторазового повторення, спочатку тестувалася система з рівними вагами (0,2 на модуль), потім поступово коригувалися залежно від внеску кожного модуля в загальну точність. Ізольований лексичний аналіз дав точність 65%. Додавання тональності підвищило до 82%, тому її вага – 0,35. Графовий аналіз збільшив до 88 % – вага 0,20. Невербальні маркери та контекст додали по 3% – по 0,15. Поріг 0,6 оптимізовано за балансом точності та помилок [6].

Точність 94% оцінювалася за стандартною метрикою F1-score на тестовому наборі з 1200 діалогів (60% – токсичні, 40% – нейтральні), анотованих трьома незалежними експертами (міжаннотаторська узгодженість Cohen's к = 0.87). F1-score враховує як точність (precision – частка правильних токсичних серед позначених), так і повноту (recall – частка знайдених токсичних серед усіх). Система досягла precision = 95%, recall = 93%, F1= 94%. Порівняно з базовою моделлю BERT для української мови, ToxDialHybrid показав на 9% вищу точність при вдесятеро меншій затримці [5].

Система працює автономно, без підключення до мережі інтернет чи зовнішніх ресурсів. Лексичний аналіз – найбільш ефективний, графовий потребує більше обчислень через мережу, але загалом забезпечує обробку десятків діалогів за секунду. Анонімізація реалізовано через вектори ознак (тональність, активність, роль) та хешування текстів. Оригінальний вміст не зберігається. Доступ ролевий, модератор бачить статистику, адміністратор – повний лог. Підхід відповідає GDPR (ст. 25, 5) та рекомендаціям щодо DPIA та згоди [4].

Тестування проводилося поетапно, від окремих модулів до навантаження на реальних діалогах з Telegram, Viber, Facebook. Увага приділена сарказму, мікроагресії, тиску. Дані оброблено етично, справедлива оплата, різноманітні аннотатори, конфіденційність, підтримка [7, 8].

ToxDialHybrid готов до інтеграції через API, обробляє до 50 діалогів за секунду з точністю 94%. Автоматизація скорочує час модерації на 72%.

Аналіз джерел сформував визначення токсичності як комбінації образ, сарказму, мікроагресії та тиску. Приклад мікроагресії «Мабуть, ти з села, якщо так пишеш», сарказм – 61% прихованого. Тиск від чотирьох + учасників змушує 31 % залишити спільноту [10, 11].

Лексика має низьку вагу через 35% прямих образ [12]. Тональність ключова (65% сарказму) [3]. Невербальні маркери – у 78% імпліцитної токсичності [3]. Контекст підвищує повноту на 12% [6].

Перспективи подальших досліджень, інтеграція з Telegram Bot, аналіз голосу, веб-панель, до навчання. Гібридні підходи виявились оптимальні для української мови.

ToxDialHybrid – ефективне рішення для виявлення токсичного контенту в українських діалогах. Гібридний підхід забезпечує точність 94% та швидкість для реального часу. Система враховує текст, структуру, невербальні елементи та контекст. Автономність, захист даних та пояснення результатів – ключові переваги. Тести підтвердили стабільність. Автоматизація зменшує навантаження модераторів і підвищує безпеку спільнот. Подальший розвиток пов'язаний з розширенням платформ, мультимедіа та адаптацією до нових форм спілкування.

Список використаних джерел

1. Efficient Toxicity Detection in Gaming Chats // arXiv. – 2025. – URL: https://arxiv.org/pdf/2510.17924
2. Toxic Content Detection in Online Social Networks // PROPOR 2024. – URL: https://aclanthology.org/2024.propor-1.48.pdf
3. SafeSpeech: Tool for Toxicity Analysis // NAACL 2025. – URL: https://aclanthology.org/2025.naacl-demo.31.pdf
4. Toxicity Detection in Ukrainian // CEUR-WS. – 2025. – URL: https://ceur-ws.org/Vol-3909/Paper_6.pdf
5. Toxicity Classification in Ukrainian // arXiv. – 2024. – URL: https://arxiv.org/pdf/2404.17841
6. Contextual BERT for Toxicity // ResearchGate. – 2025. – URL: https://www.researchgate.net/publication/390034141
7. Toxicity detection for non-mainstream languages // Toloka AI Blog. – 2025. – URL: https://toloka.ai/blog/toxicity-detection-for-non-mainstream-languages-why-we-still-need-human-labeled-data/
8. Toxic Chat Detection Using Hybrid BERT // BIS 2025. – URL: https://toknowpress.net/ISBN/978-961-6914-20-8/117.pdf
9. Toxicity Classification in Ukrainian // WOAH 2024. – URL: https://aclanthology.org/2024.woah-1.19.pdf
10. CoSyn: Implicit Hate Speech // EMNLP 2023. – URL: https://aclanthology.org/2023.findings-emnlp.XXX.pdf
11. Conversational Context in Toxicity // MSc Thesis. – 2024. – URL: http://nlp.cs.aueb.gr/theses/axenos_msc_thesis.pdf
12. Evaluating ChatGPT for Hate Speech // LREC 2024. – URL: https://aclanthology.org/2024.lrec-main.564.pdf
13. Python Web Development: Flask Guide. – Odesa: NULAw, 2024.
14. Іваненко С. О. Автоматизація модерації контенту // Цифрова економіка. – 2025. – №2.

Ключові слова: модерація контенту, токсичний контент, українські онлайн-спільноти, автоматизований аналіз діалогів, виявлення сарказму, гібридні алгоритми, обробка природної мови.

Keywords: content moderation, toxic content, Ukrainian online communities, automated dialogue analysis, sarcasm detection, hybrid algorithms, natural language processing.

ГЕНЕЗИС РОЗВИТКУ 3D-ТЕХНОЛОГІЙ У МОДЕЛЮВАННІ ТА АНІМАЦІЇ

Задерейко Олександр

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Тимофєєв Михайло

студент 3-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Сучасна українська анімаційна індустрія перебуває у складному положенні: попри доступність новітніх технологій, значний творчий потенціал та велику кількість талановитих художників, аніматорів та режисерів, вона не повною мірою відповідає світовим напрямкам розвитку за рівнем технологічного виконання, пропрацювання сценаріїв та авторської виразності. Українська анімаційна індустрія відстає від провідних студій через недостатнє фінансування, слабку інтеграцію 3D-моделювання у виробничі процеси та недостатню підтримку незалежних студій та окремих авторів. У цьому контексті 3D-моделювання є надзвичайно важливим, оскільки використання 3D технологій відкриває нові можливості для підвищення якості у тому чи іншому проекті, створення візуально видатних зображень та створення кіно, ігр чи мультфільмів світової якості [1].

Тривимірне моделювання з 1980-х років застосовується у багатьох галузях: проектуванні, візуалізації архітектури, рекламі, комп'ютерних іграх, промисловому дизайні, а також у кінематографі та анімації. Ці дві окремі галузі мають велике значення, оскільки постійне застосування 3D підтримує розвиток технологій та добросовісну конкуренцію між студіями. У кіно та анімації 3D-графіка використовується для створення реалістичного зображення вигаданих світів і персонажів, що живуть у них, задля створення відчуття правдоподібності вигаданої історії. Окрім цього, 3D-графіка також використовується для того щоб відтворити події або ефекти, які було б неможливо або занадто дорого зробити у реальному житті [2].

Щодо анімаційної індустрії: тривалий час великі анімаційні студії нехтували використанням 3D технологій у своїх роботах, покладаючись на застарілі методи 2D-анімації. Проте все змінилось після виходу "Історії Іграшок" 1995-го року - першого повнометражноно анімаційного мультфільму, повністю створеного у 3D-середовищі, який набув значного комерційного успіху і став прикладом для інших великих студій. Паралельно з цим 3D

технології або CGI також використовували у створенні фільмів. Прикладами успішних фільмів, що використовували комп'ютерну графіку є "Космічна Одисея", "Зоряні Війни", "Парк Юрського Періоду", "Володар Перстнів" та багато інших.

З 1995 року технології продовжували безперервно розвиватися. Чим потужнішими та доступнішими ставали обчислювальні можливості комп'ютерів, тим реалістичнішою могла бути 3D-анімація [3]. Особливо багато уваги приділялось фотореалізму у анімації, від чого мультфільми почали виглядати гарно, але майже одноманітно. Це помітно на прикладі студії The Walt Disney Company: їх проекти з кожним роком ставали все більш проривним з точки зору технологічності, але їх проекти створювали тиск на стандарти анімаційної індустрії, які губили авторські ідеї і різноманіття анімації серед інших великих студій.

Загалом, початок використання 3D-графіки в анімації з кінця 1980-х років пов'язаний з розвитком технологій рендерінгу та алгоритмів освітлення. Згодом, після появи алгоритмів глобального освітлення, фізично-коректних матеріалів та технології трасування променів змінились підходи до освітлення, матеріалів та композиції кадру. Нові, на той час, потужні процесори прискорювали рендеринг і зробили доступним візуально складніші сцени для більшості студій. Тому у 2000-х та 2010-х роках тенденція на покращення рендерінгу і фізики руху у проектах продовжувалась і черговими прикладами видатної, з точки зору технологій, анімації стали "Добрий Динозавр" 2015-го року, "Як приборкати дракона 3: Прихований світ" 2019-го року та "Історія Іграшок 4" 2019-го року.

Однак тенденції на фотореалізм почали змінюватись після виходу мультфільму "Людина-Павук: Навколо Всесвіту" у 2018 році: цей мультфільм став прикладом для всієї індустрії анімації у США і усього світу. Згодом у 2019 році вийшли такі проекти як "Клаус" та серіал "Аркейн", що використовували сучасні анімаційні рушії та 3D у поєднанні з 2D, створивши свої унікальні та впізнавальні стилі. На момент 2025 року попит на нові експериментальні мультфільми досі зростає по всьому світу. Мультфільми з унікальним стилем протягом останніх семи років регулярно досягають фінансового успіху, тоді як мультфільми, створені "традиційним" методом 3D із типовими сюжетами щороку все частіше зазнають провалів у прокаті. Зі сценарної точки зору це може бути пов'язано з тим, що експериментальним мультфільмам приділяється більше уваги та їм дається більше часу та творчої свободи, а отже, різні автори мають змогу розкривати особисті теми, і тому команда, яка працює над проектом, має мотивацію зробити свою роботу якомога якісніше.

У кінематографічній індустрії 3D технології виступають скоріше інструментом, а не творчим рішенням тоді як у ігровій індустрії, при розробці ігор - вибір між 3D та 2D часто є не лише творчим, але й технологічним

рішенням, оскільки певні жанри можна реалізувати лише у тривимірному просторі, а інші - лише у двовимірному. Прикладами жанрів, які повноцінно можна реалізувати лише у 3D є: “шутери”, професійні змагальні ігри, ігри з відкритим світом, ігри від третьої особи, гоночні симулятори, “Action-Adventure” з відкритим світом, стратегії у реальному часі та 3D-платформери. Всі інші жанри повністю або частково практичніше розробляли використовуючи двовимірний простір. І оскільки зараз розробка відеоігор доступна багатьом людям, як і 3D, зараз, навіть в Україні, існує багато самостійних чи невеликих незалежних груп розробників, яких, зазвичай, називають “інді розробниками”. У світі успішними іграми, що використовували 3D технології стали Minecraft, Subnautica, Risk of Rain 2, Satisfactory та багато інших. Українцям, у свою чергу, відомі такі серії ігор як “S.T.A.L.K.E.R.” та “METRO”, що також отримали світову популярність. Тому можна сказати що відеоігрова індустрія в Україні є та поступово розвивається.

Сучасний стан індустрії анімації в Україні

В історії незалежної України був лише один єдиний успішний мультфільм - Мавка“: Лісова пісня”. Він перебував у виробництві понад сім років, і вийшов у кінотеатрах та стрімінгових сервісах у 2023 році. При розробці мультфільму використовувались сучасні на той час методи 3D-моделювання і анімації, але не враховувалися світові тенденції до створення більш оригінальних та міжнародно орієнтованих проектів. У світовому прокаті “Мавка: Лісова пісня” зібрала 20 мільонів доларів, і для України це значний крок, але у порівнянні зі світовими лідерами - це занадто малий результат, хоча на сам мультфільм, витратили менш ніж 5 мільйонів доларів за інформацією з відкритих джерел [4].

Якщо народ України та вся анімаційна індустрія прагне досягти світового рівня у створенні анімації, то професійне 3D суспільство повинно звертати увагу на світові тенденції та важливість нових оригінальних ідей, які будуть зрозумілі глядачам інших країн. Підтримка оригінальних авторів, сценаристів та незалежних студій, з появою добросовісної конкуренції буде сприяти появленню нових оригінальних мультфільмів, які зададуть новий стандарт для усієї української анімаційної індустрії.

Висновки

У висновку можна сказати, що застосування 3D-моделювання у різних галузях є дуже поширеним, оскільки 3D-технології надають великі можливості як у анімації та дизайні, так і у архітектурі, кінематографі, та у створенні відеоігор. З 1980-х років розвиток 3D загалом тяжів до технологічного розвитку та створення фотореалістичних зображень, через що анімація ставала більш схожою на кіно. Такі мультфільми к “Людина-Павук: Навколо Всесвіту”, “Клаус”, серіал “Аркейн”, “Кіт у чоботях: Останнє бажання”, “Мітчелли проти машин”, “Дикий Робот” та багато інших мультфільмів, що

вийшли з 2018 року, поступово змінювали підхід цілої індустрії до створення нових мультфільмів. Люди по всьому світу зараз цікавляться оригінальною і експериментальною анімацією, яка, найчастіше, поєднує 3D і 2D, створюючи унікальний художній стиль та розповідає захопливу історію, зрозумілу глядачам зі всього світу. Для того щоб індустрія анімації в Україні досягла подібного рівня, народ і влада України повинні надати фінансові та юридичні можливості незалежним студіям для створення власних анімаційних проектів, стимулюючи добросовісну конкуренцію між усіма студіями.

Список використаних джерел:

1. Олексійчук К. О. Розробка 3D моделі персонажа для мультфільму. – 2025.
2. Гребенюк І. В., Басараба В. М., Левицька Р. Р. Сучасні тенденції в графічному дизайні: взаємодія естетики та технологій. – 2025.
3. Кобзев І., Курбін П. Створення 3d product animation для промоції продукту. – 2025.
4. Тимощук Н. М. ПЕРЕКЛАДАЦЬКІ РІШЕННЯ В АНІМАЦІЙНОМУ ФІЛЬМІ «МАВКА. ЛІСОВА ПІСНЯ» //Наукові записки. Серія: Філологічні науки. – 2025. – №. 212. – С. 242-246.

Ключові слова: генеративний ШІ.
Keywords: generative AI.

ОСОБЛИВОСТІ ЗАХОДІВ КІБЕРБЕЗПЕКИ У РЕСТОРАННІЙ СФЕРІ

Разінкін Нікіта

аспірант кафедри статистики та ММЕ Одеського національного економічного університету

Нгуен Фиок Бао Шон

студент факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сфері ресторанного бізнесу, яка є невід'ємною частиною індустрії гостинності, заходи кібербезпеки набувають особливого значення через швидку цифровізацію процесів, що включає обробку персональних даних клієнтів, управління системами точок продажу та інтеграцію з онлайн-платформами для замовлень і доставки. Така цифрова трансформація, з одного боку, сприяє підвищенню ефективності та персоналізації послуг, а з іншого – створює численні вразливості, які експлуатуються кіберзлочинцями для отримання доступу до конфіденційної інформації, такої як дані кредитних карток, адреси електронної пошти та контактні номери. Як науковець, що спеціалізується на аналізі ризиків у сфері послуг, я підкреслюю, що ресторанний сектор стикається з унікальними викликами, пов'язаними з

високим оборотом персоналу, обмеженими ресурсами на впровадження складних систем захисту та залежністю від постачальників третіх сторін, що часто призводить до ланцюгових порушень. Згідно з аналізом, проведеним у контексті стійких систем послуг, ключовими зацікавленими сторонами є клієнти, співробітники, постачальники, акціонери, регулятори, конкуренти та медіа, кожен з яких по-різному впливає на рівень ризику та відповідальності за його мінімізацію. Наприклад, регулятори відіграють домінуючу роль у встановленні норм, тоді як клієнти та співробітники є найбільш залежними від ефективності заходів захисту [1].

Серед основних кіберзагроз у ресторанній сфері виділяються фішингові атаки, порушення даних, програми-вимагачі, атаки на відмову в обслуговуванні та системні вразливості, які часто кореняться в людському факторі, застарілих технологіях та слабких ланцюгах постачання. Фішинг, як одна з найпоширеніших тактик, передбачає обман співробітників або клієнтів через фальшиві електронні листи чи повідомлення, що призводить до витоку даних або встановлення шкідливого ПЗ, і є причиною багатьох подальших порушень, таких як крадіжка даних кредитних карток у системах POS. Порушення даних, у свою чергу, являють собою несанкціонований доступ до конфіденційної інформації, як це сталося в випадку з великими мережами ресторанів, де витік стосувався мільйонів клієнтів, включаючи імена, номери соціального страхування та фінансові деталі, що спричинило не лише фінансові втрати, але й втрату довіри. Програми-вимагачі блокують доступ до критичних систем, таких як бази даних замовлень чи інвентарю, вимагаючи викуп, і часто призводять до тимчасового закриття закладів, як у випадку з майже 300 ресторанами у Великобританії, де атака спричинила хаос у операціях. Атаки DoS перевантажують сервери, роблячи сайти чи системи замовлень недоступними, що особливо шкідливо для ресторанів з онлайн-присутністю, тоді як системні вразливості, такі як незахищені Wi-Fi чи неоновлені POS-термінали, служать точками входу для хакерів, експлуатуючи слабкості в апаратному чи програмному забезпеченні [1,2].

Конкретні приклади порушень у ресторанній сфері ілюструють серйозність проблеми та необхідність адаптованих заходів. Наприклад, у 2015 році атака на мережу Hilton торкнулася POS-систем у ресторанах і магазинах готелів, викравши дані 350 тисяч кредитних карток, включаючи імена, коди безпеки та терміни дії, що призвело до штрафу в 700 тисяч доларів через затримку в реагуванні. Аналогічно, порушення в Wyndham Hotels з 2008 по 2010 рік зачепили понад 619 тисяч записів клієнтів, включаючи кредитні картки, спричинивши шахрайство на суму понад 1,6 мільйона доларів і значні юридичні витрати. У ресторанному сегменті, як у випадку з великими мережами швидкого харчування, атаки часто починаються з несанкціонованого доступу до електронної пошти співробітників, що дозволяє

хакерам збирати облікові дані та проникати глибше в мережу, експлуатуючи високий оборот персоналу та низьку обізнаність з кібербезпеки. Ці інциденти підкреслюють, що наслідки включають не лише безпосередні фінансові втрати, але й репутаційні збитки, судові позови та операційні перебої, які можуть тривати дні чи тижні, особливо в умовах, коли близько 80% транзакцій у ресторанах є цифровими [2,3].

Для ефективного протистояння цим загрозам у ресторанній сфері необхідне впровадження комплексних заходів, що охоплюють як технічні, так і організаційні аспекти. Серед ключових практик – регулярне навчання персоналу з розпізнавання фішингу та соціальної інженерії, оскільки людський фактор є причиною більшості порушень, і це вимагає постійних сесій, враховуючи високий оборот кадрів у швидкому обслуговуванні. Важливим є впровадження багатофакторної аутентифікації для всіх систем, сильних політик паролів, що включають комбінацію символів, цифр і букв, та обмеження доступу до чутливої інформації на основі ролей співробітників, аби мінімізувати внутрішні загрози від недбалості чи зловмисності. На технічному рівні рекомендується проводити регулярні оцінки вразливостей, оновлення програмного забезпечення та апаратного забезпечення, шифрування даних у POS-системах від кінця до кінця, щоб запобігти перехопленню під час передачі, а також розділення гостьових Wi-Fi мереж від внутрішніх для уникнення витоків через незахищені з'єднання. Крім того, створення планів реагування на інциденти, що включають крос-функціональні команди з IT-спеціалістів, керівництва та юристів, дозволяє швидко локалізувати порушення, повідомляти зацікавлених сторін і відновлювати операції, зменшуючи витрати на відновлення. Управління ризиками третіх сторін, такими як постачальники доставки чи платформи бронювання, вимагає ретельної перевірки їхніх стандартів безпеки та регулярних аудитів, оскільки порушення в ланцюгу постачання, як у випадку з Marriott-Starwood, можуть поширитися на весь бізнес [3,4,5].

Додатково, для стійкості ресторанного бізнесу до кіберзагроз варто впроваджувати резервне копіювання даних у хмарних сховищах, відокремлених від основної мережі, аби швидко відновлюватися після атак вимагачів, та використовувати інструменти моніторингу в реальному часі для виявлення аномалій, що скорочує час перебування зловмисників у системі, який у цій галузі може перевищувати рік. З точки зору стійких систем, аналіз за допомогою методів, таких як PFSs-MACTOR, показує, що посилення регуляторних норм, таких як PCI DSS для платежів чи GDPR для даних, є критичним для координації зусиль усіх стейкхолдерів, де регулятори домінують у встановленні стандартів, а співробітники та клієнти потребують підвищення обізнаності для протидії фішингу як кореневій причині багатьох ризиків. У контексті швидкого харчування та роздрібної торгівлі продуктами

харчування, де цифрова взаємодія з клієнтами через додатки лояльності та кіоски самообслуговування є нормою, акцент на шифруванні чутливих даних і регулярних тестах безпеки стає невід'ємним для запобігання хаосу в операціях [1,4].

Нарешті, ефективність заходів кібербезпеки в ресторанній сфері залежить від створення культури безпеки, де керівництво з верхівки до низу інтегрує захист як щоденну практику, поєднуючи з інноваціями, такими як штучний інтелект для виявлення аномалій і прогнозування загроз. Це не лише мінімізує фінансові та репутаційні втрати, але й сприяє стійкому розвитку індустрії, забезпечуючи довіру клієнтів у цифрову епоху.

Список використаних джерел

1. Karadayi-Usta S. Cybersecurity Risks Analysis in the Hospitality Industry: A Stakeholder Perspective on Sustainable Service Systems. *Systems.* 2024. №12(10):397. DOI: https://doi.org/10.3390/systems12100397
2. Elgan M. The rising threat of cyberattacks in the restaurant industry. IBM. URL: https://www.ibm.com/think/news/rising-threat-cyberattacks-restaurant-industry (дата звернення: 30.10.2025).
3. Chin K. Cybersecurity in the Hospitality Industry: Challenges and Solutions. UpGuard. URL: https://www.upguard.com/blog/cybersecurity-in-the-hospitality-industry (дата звернення: 30.10.2025).
4. Cybersecurity Best Practices for Food Retailers and QSR. NSF. URL: https://www.nsf.org/knowledge-library/cybersecurity-best-practices-for-food-retailers-and-qsr (дата звернення: 30.10.2025).
5. Pollak N. Cybersecurity for restaurants: 7 common risks and how to avoid them. Cloud Kitchens. URL: https://cloudkitchens.com/blog/cybersecurity-for-restaurants/ (дата звернення: 30.10.2025).

Ключові слова: кібербезпека, POS-системи, фішингові атаки, багатофакторна аутентифікація, шифрування даних, управління ризиками, цифровізація.
Keywords: cybersecurity, POS systems, phishing attacks, multi-factor authentication, data encryption, risk management, digitalization.

СИСТЕМНИЙ АНАЛІЗ ТА ОПТИМІЗАЦІЯ ЕФЕКТИВНОСТІ ВЕБПОРТАЛУ НА ОСНОВІ ПОВЕДІНКИ КОРИСТУВАЧА

Куклінова Софія

студентка факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасних реаліях вебпортали виступають не лише засобом представлення інформації, а й ключовим інструментом інформаційного обміну, комунікації та взаємодії між користувачами і цифровими сервісами. Від

ефективності їхньої роботи, зручності навігації та якості користувацького досвіду залежить рівень залучення, лояльність аудиторії та конкурентоспроможність. Розвиток інструментів аналітики, зокрема Google Analytics 4, дає змогу аналізувати поведінкові патерни користувачів, виявляти слабкі місця у структурі сайту та прогнозувати реакцію відвідувачів на контент [1].

Метою роботи є комплексна розробка та аналітичне обґрунтування підходів до системного аналізу й оптимізації вебпорталу на основі поведінкових метрик користувачів і сучасних інструментів вебаналітики. Об'єктом дослідження виступає процес оптимізації ефективності інтерактивного вебпорталу для рецензування відеоігор, розробленого на базі фреймворку Django з використанням архітектури MVT [2]. Методика дослідження базується на поєднанні системного аналізу, емпіричних спостережень, інструментальної вебаналітики та моделювання даних.

Теоретичний аналіз показав, що вебпортали є складними інформаційно-комунікаційними системами, що поєднують технологічну платформу, базу даних, програмну логіку та інтерфейс користувача [3]. Для оцінювання ефективності використовують систему метрик, які поділяють на технічні, поведінкові та бізнес-метрики. До технічних метрик відносяться час завантаження, uptime та мобільна адаптивність. Поведінкові метрики включають показник відмов, середню тривалість сесії, глибину перегляду та конверсію. Бізнес-метрики охоплюють ROI, CPA та Retention Rate [4].

Наукова новизна роботи полягає у розробці комплексного підходу, що поєднує методи системного аналізу, вебаналітики та імітаційного моделювання користувацької поведінки. Уперше запропоновано модель симуляції користувацького трафіку з використанням Python та інтеграції з Google Analytics 4 через Measurement Protocol, яка дозволяє формувати аналітичні дані для дослідження ефективності вебпорталу без залучення реальних користувачів.

У межах дослідження було створено експериментальне середовище, яке дало змогу імітувати поведінку користувачів, аналізувати дані та оцінювати вплив факторів на показники залученості. Для забезпечення аналітичної складової було інтегровано Google Analytics 4 через Measurement Protocol [5]. З метою формування статистично значущих даних було створено Python-скрипт симуляції користувацької активності, який моделював різні типи взаємодії: page_view, add_comment, scroll, form_start, form_submit, user_engagement, session_start, first_visit.

Для наближення симуляції до реальної поведінки було розроблено п'ять персон користувачів: Bouncer (залишає сайт після однієї сторінки), Skimmer (переглядає декілька сторінок з мінімальними діями), Deep reader (детально читає статті та залишає коментарі), Tabber (швидко перемикається між

вкладками) та Registrant (проходить повний шлях реєстрації) [6]. Загальна кількість подій склала понад 15 тисяч із 1494 унікального користувача.

На основі зібраних даних було створено аналітичні діаграми за допомогою бібліотек pandas, matplotlib і seaborn. Стовпчаста діаграма подій показала, що користувачі найчастіше переглядають сторінки (70,3% усіх подій), але рідко взаємодіють з формою реєстрації (2,39%). Кругова діаграма типів користувачів виявила, що більшість відвідувачів належать до пасивних типів: Skimmers становлять 35,6%, Deep Readers – 26,7%, Bouncers – 20%, Tabbers – 11,1%, Registrants – 6,7% [7].

Теплові карти відвідувань сторінок дозволили виявити найбільш популярні розділи. Найпопулярнішими виявилися категорії «Популярні ігри», «Action» та «Adventure» з 1367-2380 переглядами. Найменшу відвідуваність мали «Добірка від автора» (247 відвідувань) і «Sports» (391 відвідування). Лінійний графік показав зростання активності в середині симуляції з наступним спадом наприкінці, що вказує на необхідність механізмів утримання користувачів.

На основі аналізу було виділено ключові проблеми вебпорталу. Низький показник form_submit (2,39%) ймовірно пов'язаний з незручною формою або її непомітністю. Високий відсоток Bouncers (20%) свідчить про слабку привабливість головної сторінки. Низький scroll вказує на монотонний контент та відсутність візуальних блоків. Зменшення активності в часі показує відсутність стимулів для повернення користувачів [8].

Було здійснено теоретичну оптимізацію UX/UI без фактичного редизайну. Для головної сторінки запропоновано частіше оновлювати новини, додавати інтерактивні блоки з рекомендаціями, адаптувати навігацію під мобільні пристрої та переробити форму реєстрації. Для підвищення конверсії пропонується скорочення полів форми, підтримка автозаповнення та чітка кольорова контрастність кнопок [9].

Після моделювання змін прогнозується значне покращення показників. Показник відмов може знизитися з 20% до 12% (зміна на 40%). Середня тривалість сесії може зрости з 1,2 до 1,7 хвилин (покращення на 41%). Коефіцієнт надсилання форми може збільшитися з 2,39% до 3,5% (зростання на 46%). Кількість сторінок за сеанс може зрости з 3,1 до 4,4 (покращення на 42%). Коефіцієнт залученості може збільшитися з 58% до 74% (зміна на 27%). Кількість повернень може зрости з 18% до 28% (покращення на 55%).

Кореляційний аналіз показав найтісніший позитивний зв'язок між Engagement Rate та Return Visitors (r=0,81), між Engagement Rate та Form Submit Rate (r=0,66). Bounce Rate має сильну негативну кореляцію з усіма метриками (від -0,55 до -0,74), що підтверджує, що зменшення відмов прямо свідчить про покращення досвіду користувачів [10].

Проведене дослідження підтвердило доцільність використання системного підходу до аналізу вебпорталів. Використання Google Analytics 4 у поєднанні з Python дає змогу створити повну картину користувацької взаємодії. Розроблена модель симуляції є дієвим інструментом дослідження навіть за відсутності реальної аудиторії. Результати доводять, що аналітичні та теоретичні UX/UI-покращення здатні суттєво вплинути на показники ефективності вебпорталу, збільшуючи рівень залучення та задоволеності користувачів на 27-55%.

Список використаної літератури:

1. Куклінова С. І. Розробка інтерактивного вебпорталу для рецензування відеоігор : кваліфікаційна робота бакалавра / Куклінова Софія Іванівна ; наук. кер. [Коновалов Сергій Миколайович]. Одеса : Одеський національний морський університет, 2024. С. 33–62.
2. Романишин Ю., Крупа Х. Інформаційні сервіси інтернет-порталів фандрайзингових організацій. Цифрова платформа: інформаційні технології в соціокультурній сфері. 2024. Т. 7, № 1. С. 171–187.
3. Задорожна Н. Підходи до створення та підтримки порталів. Проблеми програмування. 2006. № 2-3. С. 569–579.
4. Rahman N., Hasda A. Y., Niswaty R. Effectiveness of the use of mail application information systems at the Center for Security and Enforcement of Environmental and Forestry Law in Sulawesi Region. International Journal of Administration and Education (IJAE). 2024. P. 29–40.
5. Samocha D. Effectiveness of web-based interventions on patient empowerment: a systematic review and meta-analysis. Journal of Medical Internet Research. 2010. Vol. 12, No. 2. Article e1286.
6. Advanced Examination of User Behavior Recognition via Log Dataset Analysis of Web Applications Using Data Mining Techniques. MDPI Journals. 2023. DOI: https://doi.org/10.3390/app13020845
7. Website Traffic Patterns and User Behavior: A Comprehensive Study of Visitor Interactions and Engagement Metrics. Innocon Journal of Digital Research. 2023.
8. Pay Attention to Web Performance Metrics to Improve the UX. UXmatters Magazine. 2022.
9. Analysis of Web Server Logs to Understand Internet User Behavior and Develop Digital Marketing Strategies. Science Publications & Communication (SciencePubCo). 2023.
10. Бубенець І. Г., Сломінцев Д. М. Сучасні аспекти цифрового маркетингу: основні показники ефективності. БізнесІнформ. 2022. № 11. С. 271–276.

Ключові слова: системний аналіз, вебпортал, користувацька поведінка, Google Analytics 4, оптимізація UX/UI, вебаналітика, метрики ефективності.

Keywords: system analysis, web portal, user behavior, Google Analytics 4, UX/UI optimization, web analytics, performance metrics.

ANALYSIS AND MODELING OF THE PLAYER'S EMOTIONAL STATES IN ADAPTIVE GAME DESIGN SYSTEMS

Chepurna Olena

Associate Professor of the Department of Cyber Security, National University «Odessa Law Academy», Candidate of Physical and Mathematical Sciences

Shliakhtytskyi Dmytro

4th year student of the Faculty of Cybersecurity and Information Technology National University «Odessa Law Academy»

In modern interactive systems, in video games, there is a constant evolution of the ways in which the user and the digital environment interact. One of the most important directions of this evolution is the development of emotional design, a concept that aims to form a certain emotional state in the player, which enhances engagement, increases the level of pleasure and creates a deeper sense of immersion in the virtual world. Emotional design in modern games is no longer limited to visual or sound effects but is based on a deep understanding of human psychological and behavioral reactions. Given the rapid development of artificial intelligence, machine learning, procedural content generation, and behavioral models, there are real prerequisites for mathematical description and algorithmic control of the emotional interaction between the player and the system.

Despite this, in the scientific and practical plane of game design, the issue of formalizing the user's emotional states remains unresolved. The complexity of the problem lies in the fact that emotions are subjective, multidimensional and dynamic, so it is difficult to describe them with a single model [1]. Most modern games use static elements of emotional design that do not respond to changes in the player's state in real time. This method restricts the possibilities for further interactivity and prevents the development of genuinely adaptive systems. Consequently, it is necessary to establish mathematical and algorithmic principles for emotional design to guarantee objectivity, predictability, and practical technological application [2].

The essence of the problem lies in the lack of a universal methodology that would combine the psychological aspects of perception with formal methods of data processing. It is necessary to create such mathematical models that can adequately reflect the change in the user's emotional states depending on the events of the game, as well as appropriate algorithms that will allow you to flexibly adapt the content. To do this, it is advisable to use methods of fuzzy logic, probability theory, Markov processes, as well as modern machine learning approaches and neural network architectures. They make it possible to identify hidden patterns in the player's behavior and predict his reactions to certain game stimuli.

The purpose of the study is to develop conceptual and practical approaches to the implementation of emotional design in game systems based on mathematical

models and algorithmic adaptation mechanisms. This approach involves creating an intellectual environment that can analyze behavioral data, assess the player's current emotional state, and dynamically change the parameters of the game to maintain the desired level of emotional involvement. For example, the system can automatically change the complexity, color scheme, musical accompaniment, or intensity of events based on an assessment of the user's emotional state.

The formalization of emotional states can be carried out by introducing quantitative parameters such as levels of pleasure, tension, interest, fear or joy. Each of these options can have a numerical representation that is updated in real time according to the user's actions. Clustering algorithms, Bayesian networks, or recurrent neural networks capable of simulating sequential changes in player behavior can be used to process such data. In this way, a model is created that not only reacts to current events, but also predicts future user reactions, providing a deeper personalization of the gaming experience.

Algorithmic support of emotional design includes several key stages: collection of game telemetry, analysis of behavioral patterns, construction of an emotional state model, and generation of appropriate content. Game telemetry covers indicators of reaction speed, press frequency, decision-making time, errors, direction of gaze, and even the rhythm of interaction. Based on this data, the system can determine the level of stress, irritation or satisfaction of the user. Pattern analysis algorithms allow you to identify moments when a player loses interest or, on the contrary, shows high engagement. The system can then change the playing conditions to maintain optimal emotional balance, prevent fatigue or frustration.

The solution to this problem is possible by integrating emotional design with machine learning algorithms that are trained on the behavioral data of a large number of users. This approach provides the formation of a knowledge base about typical emotional reactions to certain game situations. In the future, this knowledge can be used to build models that can predict the reaction of new players and automatically adjust the gameplay [3]. For example, if the system detects that the user is in a state of frustration for too long, it can reduce the complexity, change the dynamics of the music, or offer a hint. If there is a decrease in interest, the game can increase the pace of events or introduce new stimuli to restore attention.

Thus, emotional design, built on mathematical and algorithmic principles, becomes an important element of adaptive game architecture. Its implementation contributes not only to improving the quality of gameplay, but also to creating a deeper connection between the player and the digital space. Thanks to this, the game ceases to be just a set of mechanics and turns into an intelligent system capable of empathizing with the user. The development of such systems is of promising importance not only for the entertainment industry, but also for educational, psychological and rehabilitation applications, where emotional interaction plays a key role.

In the future, the development of mathematical models of emotional dynamics will make it possible to create universal tools for automatic regulation of the gaming environment. The combination of behavioral analytics, artificial intelligence, and adaptive algorithms will contribute to the formation of a new paradigm of emotionally oriented design. Further research should be aimed at improving methods for recognizing emotions based on biometrics, voice analysis, facial expressions, or keystroke patterns. An important area will be the optimization of the computational costs of such algorithms, which will ensure their effective integration into real game engines without reducing performance.

Thus, the mathematical and algorithmic foundations of emotional design form the scientific and technical foundation for a new generation of game systems capable of understanding, predicting and maintaining the emotional state of the user. The use of formal methods allows you to turn subjective emotions into a manageable parameter, which increases the effectiveness of communication between the player and the system. This approach opens new opportunities for creating intellectual, adaptive, and psychologically deep game products, where the main object of design is not only the process, but also the emotional experience of a person.

References:

1. Alkhomsan M. N. Eliciting and modeling emotional requirements. A systematic mapping review. PLoS ONE. 2024. URL. https://pmc.ncbi.nlm.nih.gov.
2. Belkacem M. Balla A. Trigano P. A generic and efficient emotion-driven approach toward personalized assessment and adaptation in serious games. Journal of Computer and Education. 2019. URL. https://www.sciencedirect.com.
3. Makantasis K. Yannakakis G. Liapis A. The Pixels and Sounds of Emotion. General-Purpose Representations of Arousal in Games. 2021. URL. https://arxiv.org.

Key words: Modeling, Emotion, Game Development.
Ключові слова: моделювання, емоція, розроблення ігор.

ДОСЛІДЖЕННЯ МЕТОДІВ АДАПТАЦІЇ ІНТЕРФЕЙСІВ ДЛЯ КОРИСТУВАЧІВ З КОГНІТИВНИМИ ПОРУШЕННЯМИ

Гура Володимир

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Вдовін Олександр

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Дослідження методів адаптації інтерфейсів користувача для осіб з когнітивними порушеннями – фокусується на створенні цифрових систем (веб-

сайтів, додатків), які враховують обмеження уваги, пам'яті та обробки інформації. Когнітивні порушення це стани, коли людина має труднощі з пам'яттю, увагою, прийняттям рішень або обробкою інформації, наприклад деменція (втрата когнітивних функцій через хворобу), синдром дефіциту уваги з гіперактивністю (коли важко зосередитися), інтелектуальні вади (обмежена інтелектуальна здатність від народження) чи легкі когнітивні порушення (перехідний стан до деменції). За даними Всесвітньої організації охорони здоров'я, когнітивні порушення впливають на значну частину населення світу через старіння [1]. В Україні когнітивні порушення торкаються переважно літніх людей та дітей шкільного віку з синдромом дефіциту уваги з гіперактивністю [2]. Користувачі покладаються на спрощений дизайн, оскільки складні інтерфейси викликають фрустрацію та відмову від використання [3]. Напрямок дослідження базується на принципах універсального дизайну, де інтерфейс адаптується без зовнішніх пристроїв, використовуючи HTML, CSS, JavaScript та стандарти WCAG (Web Content Accessibility Guidelines, міжнародні рекомендації з доступності, версія 2.2 додає критерії для когнітивних вад) [4]. Спрощення тексту підвищує розуміння для осіб з легкими когнітивними порушеннями [5].

В Україні значна кількість осіб мають когнітивні порушення, переважно люди літнього [2]. Більшість державних сайтів не відповідають WCAG 2.2 AA для когнітивної доступності, що призводить до виключення частини населення з цифрового кола послуг [7]. Закон України та Постанова КМУ № 1234 вимагають повної доступності населення до цифрового простору до 2026 року [8]. На міжнародному рівні аналіз мільйона найпопулярніших домашніх сторінок веб-сайтів показує, що переважна більшість з них містить помилки, пов’язані з когнитивною доступністю [7]. Багато українців зазнають впливу когнітивних проблем через стрес війни, посттравматичний синдром та старіння [1]. Когнітивні порушення збільшують час виконання завдань, користувачі з деменцією витрачають значно більше часу на заповнення простих веб-форм [6]. Проста адаптація підвищує самостійність, зменшує залежність від опікунів та юридичні ризики [3]. Більшість українських розробників працюють без AI [9], тому прості методи на базі HTML/JS актуальні для малого бізнесу та держ. порталів. Без адаптації сайти електронної комерції втрачають значну частину продажів від користувачів з когнітивними порушеннями [10].

Багато рішень пропонують складні моделі адаптації інтерфейсів, такі як навчання з підкріпленням (метод, де модель вчиться через винагороди та покарання) та Інтернет речей (мережа підключених пристроїв з датчиками), які недоступні через високу вартість, велику складність впровадження, потребу в значних обсягах даних та відсутність відповідних навичок у більшості розробників [9]. Неточність полягає в тому, що переважна більшість

сайтів не відповідає вимогам WCAG щодо когнітивних недоліків [7], оскільки розробники зосереджуються переважно на візуальних аспектах, ігноруючи спрощення тексту чи уникнення елементів, що відволікають увагу. Невизначеність проявляється у відсутності простих локальних адаптацій, які працюють без серверів, через що такі рішення стають непридатними для України, зокрема для малого бізнесу та державних порталів [7]. Дослідження демонструють, що моделі штучного інтелекту для спрощення тексту вимагають великої кількості прикладів українською мовою, яких наразі недостатньо [11]. Фрагментарність існуючих рішень проявляється в тому, що окремі плагіни охоплюють лише частину критеріїв WCAG 3.1.5 [4, 11, 12]. Це означає, що жоден з них не забезпечує комплексного покриття всіх аспектів когнітивної доступності, таких як спрощення тексту, уникнення відволікаючих елементів та динамічну адаптацію під користувача. В результаті розробники змушені комбінувати кілька інструментів, що ускладнює впровадження та підвищує ризик несумісності. Такий підхід не відповідає принципам універсального дизайну та залишає значну частину бар'єрів неусуненими.

Переваги розробленої системи адаптації веб-інтерфейсів для користувачів з когнітивними порушеннями над існуючими підходами наведено у табл. 1:

Таблиця 1. Порівняння системи адаптації веб-інтерфейсів для користувачів з когнітивними порушеннями системи з існуючими рішеннями

Критерій впровадження	Розроблена система	Складні моделі ШІ	IoT-рішення	Переваги	Недоліки	Приклад використання
Вартість впровадження	Низька (лише HTML/JS)	Висока	Висока	Не потребує бюджету на обладнання	Вимагає значних інвестицій	Держ. портали, малий бізнес
Час впровадження	Кілька днів	Тижні	Місяці	Швидке розгортання без навчання	Довгий цикл розробки та тестування	Diia.Osvita, банки
Потрібні дані	Ні	Так	Так	Повна конфіден-ційність	Ризик витоку даних	Локальні сайти без серверів

Залежність від серверів	Ні	Так	Так	Працює офлайн	Неможливо в регіонах з обмеженим зв'язком	Регіональні портали
Доступність для України	Висока	Низька	Низька	Розробник може впровадити без ШІ	Лише великі компанії з ресурсами	Малий бізнес, стартапи
Відповідність WCAG 2.2	Повна	Часткова	Часткова	Покриває когнітивні критерії (3.1.5, 3.3.8)	Ігнорує спрощення тексту	Освітні платформи
Ефект для користувачів	Швидше виконання завдань	Високий, але з помилками	Високий	Менше помилок і відмови	Відмова від використання	Користувачі з деменцією

Як видно з таблиці 1, розроблена система усуває ключові бар'єри – високу вартість, залежність від серверів і потребу в даних – роблячи адаптацію доступною для українських розробників. Це ідеально відповідає реаліям малого бізнесу, державних порталів і регіонів з обмеженим доступом до інтернету.

Система адаптації інтерфейсів розпочинається з короткого опитування на початку роботи з сайтом або додатком, яке містить кілька простих питань, наприклад, чи важко користувачеві читати довгі тексти, чи потрібні йому великі кнопки, чи відволікають увагу анімаційні елементи. Відповіді зберігаються в локальному сховищі браузера без використання серверів, що дозволяє визначити спрощений режим роботи. Спрощення тексту відбувається за допомогою індексу читабельності Флеша (математична формула, розроблена Рудольфом Флешем, яка оцінює, наскільки текст легко читати та розуміти. Вона базується на довжині речень і слів, чим коротші речення та чим менше складів у словах – тим вищий бал, який передбачає використання коротких речень, простих слів, наприклад, заміну слова "використовуйте" на "натисніть", а також вимикання анімацій за допомогою медіа-запиту для зменшення руху та збільшення розміру кнопок. Загальні правила адаптації полягають у тому, що при частому поверненні користувача назад або тривалому перебуванні на формі автоматично додаються текстові підказки з використанням атрибута для динамічного оголошення змін. Елементи дизайну для легкого розуміння становлять комплекс візуальних, структурних та

інтерактивних рішень, спрямованих на зменшення когнітивного навантаження для осіб з порушеннями уваги, пам'яті чи сприйняття. Кожен елемент базується на критеріях рівня відповідності WCAG 2.2 AA, результатах тестувань з реальними користувачами, зручності використання та практичних рекомендаціях міжнародної організації зі стандартизації веб-технологій [3, 4].

Текст залишається основним джерелом інформації, однак складні конструкції перенавантажують робочу пам'ять, тому рекомендується підтримувати індекс читабельності Флеша не нижче стандартного рівня, що досягається за допомогою коротких речень, активного стану, простих слів та уникнення абстракцій. Технічна реалізація включає обробку текстового вмісту сторінки після завантаження сторінки або залежно від профілю користувача, при цьому система автоматично скорочує довгі речення та замінює складні слова на простіші синоніми з локального словника. Користувачі з когнітивними порушеннями потребують чіткої орієнтації, тому кожен екран має єдину логічну послідовність від загального до конкретного. Технічна реалізація передбачає використання навігаційних шляхів у вигляді впорядкованого списку з семантичною розміткою навігації та візуальними роздільниками, а кнопка повернення фіксується в лівому верхньому куті та залишається доступною під час прокручування, що забезпечує передбачуваність і зменшує дезорієнтацію. Моторні та когнітивні помилки зменшуються завдяки достатньому розміру зон натискання, для чого технічна реалізація застосовує мінімальні значення висоти та ширини для всіх інтерактивних елементів через каскадні таблиці стилів з відступами для зручності, а також додає іконки для візуально-мовного дублювання. Контраст між текстом і фоном має бути достатнім, при цьому інформація не повинна передаватися виключно кольором. Технічна реалізація включає автоматичний режим високого контрасту залежно від профілю з перевизначенням змінних каскадних таблиць стилів для фону, тексту та акцентів, а перевірка контрасту інтегрується в процес розробки за допомогою інструментів наприклад, за допомогою інструментів типу Lighthouse (безкоштовний інструмент з відкритим кодом від Google).

Анімації, автоматичне прокручування та спливаючі вікна переривають увагу, тому технічна реалізація вимикає анімації та переходи залежно від профілю або системних налаштувань для зменшення руху, зупиняє відео з автоматичним відтворенням і робить динамічні елементи статичними. Усе інтерактивне повинно бути доступним через клавіатуру з логічним порядком від гори до низу та зліва направо, для чого технічна реалізація забезпечує видимий фокус через обведення при фокусі клавіатурою. Посилання для пропуску дозволяють швидко перейти до основного контенту та видимі лише при фокусі, а мікроінструкції розміщуються біля полів, для чого технічна реалізація додає підказки. При тривалому фокусі на елементі з'являється динамічна підказка. Кожен екран містить шапку з логотипом і навігацією,

основний контент в одній колонці та підвал, для чого технічна реалізація використовує семантичні ролі шапки, навігації, основного блоку та інформації. У спрощеному режимі видаляються бічні панелі та обмежується ширина контенту. Автоматичне тестування проводиться за допомогою axe-core (безкоштовна бібліотека з відкритим кодом від Deque Systems, яка автоматично перевіряє веб-сторінки на відповідність стандартам доступності (WCAG)) та Lighthouse CI (безкоштовний інструмент від Google для автоматичного тестування веб-сайтів на доступність, швидкість та SEO у процесі розробки (CI/CD)), а ручне – з реальними користувачами. Показники включають час до завершення завдання, кількість помилок та оцінку за шкалою зручності використання. Ці елементи формують єдину систему легкого розуміння, яка технічно реалізована, відповідає стандартам і працює для користувачів з когнітивними порушеннями без додаткового обладнання з швидким впровадженням. [4-6,12]

Доступність системи адаптації веб-інтерфейсів для користувачів з когнітивними порушеннями, полягає в тому, що вона працює на будь-якому сайті, побудованому на HTML та JavaScript. Безпека забезпечується зберіганням даних виключно локально в браузері без будь-якого стеження. Масштабованість дозволяє швидко інтегрувати рішення в WordPress, React чи інші платформи. Економічна ефективність досягається завдяки низькій вартості впровадження. Відповідність стандартам WCAG охоплює ключові критерії – контраст, клавіатурна навігація, читабельність тексту – і усуває основні когнітивні бар'єри. Проста система, що поєднує профіль користувача, правила адаптації та вимоги WCAG, ефективно спрощує інтерфейси для осіб з когнітивними порушеннями впроваджується за кілька днів, не потребує штучного інтелекту чи датчиків і суттєво скорочує час виконання завдань. Вона ідеально підходить для України – державних порталів, банківських систем, освітніх платформ (наприклад, Diia.Osvita). Рекомендація полягає в тому, щоб почати з опитувальника користувача та спрощення тексту – це дасть максимальний ефект при мінімальних зусиллях.

Список використаних джерел:

1. World Health Organization, "Dementia fact sheet," 2023. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/dementia
2. Міністерство охорони здоров'я України, "Стан психічного здоров'я населення України," 2025. [Online]. Available: https://moz.gov.ua
3. Level Access, "WCAG 2.2 AA Summary and Checklist," 2025. [Online]. Available: https://www.levelaccess.com/blog/wcag-2-2-aa-summary-and-checklist-for-website-owners/
4. W3C, "Web Content Accessibility Guidelines (WCAG) 2.2," 2023. [Online]. Available: https://www.w3.org/TR/WCAG22/

5. L. Moreno, P. Martínez, B. Ruiz-Mezcua, and A. Iglesias, "Designing user interfaces for content simplification in older adults with cognitive impairments," Universal Access in the Information Society, 2024, doi: 10.1007/s10209-023-01078-5.
6. A. Esposito, M. Amoretti, and M. Vallone, "Advancing Accessible Interfaces for Cognitive Disabilities," in Proc. DSAI 2024, 2024.
7. WebAIM, "The WebAIM Million: An annual accessibility analysis of the top 1,000,000 home pages," 2025. [Online]. Available: https://webaim.org/projects/million/
8. Кабінет Міністрів України, "Постанова № 1234 'Про затвердження вимог до цифрової доступності'," 2024. [Online]. Available: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-vymog-do-tsifrovoyi-dostupnosti
9. DOU, "Рейтинг мов програмування та технологій в Україні," 2025. [Online]. Available: https://dou.ua/lenta/articles/programming-languages-2025/
10. Deque Systems, "Axe DevTools: Accessibility Testing Tools," 2025. [Online]. Available: https://www.deque.com/axe/devtools/
11. A. Gupta and R. Singh, "AI-enhanced digital therapeutics for cognitive impairments," Discover Artificial Intelligence, vol. 5, no. 1, pp. 1–15, 2025, doi: 10.1007/s44163-025-00325-6.
12. W3C, "ARIA Authoring Practices Guide (APG)," 2025. [Online]. Available: https://www.w3.org/WAI/ARIA/apg/

Ключові слова: когнітивні порушення, доступність інтерфейсів, універсальний дизайн, когнітивна доступність, WCAG 2.2, спрощення тексту, адаптація користувацьких інтерфейсів.
Keywords: cognitive impairments, interface accessibility, universal design, cognitive accessibility, WCAG 2.2, text simplification, user interface adaptation.

КОМУНІКАЦІЙНІ СТРАТЕГІЇ ПРОТИДІЇ РЕПОСТАМ І «ДЗЕРКАЛАМ» МУЛЬТИМЕДІЙНОГО КОНТЕНТУ: ВЗАЄМОДІЯ З ПЛАТФОРМАМИ ТА СПІЛЬНОТАМИ

Овчинников Микола
асистент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Поширення мультимедійних даних у кіберпросторі дедалі частіше супроводжується повторними завантаженнями, репостами та створенням «дзеркал» контенту, що ускладнює практичний захист прав правовласника. У межах дисертаційного дослідження з розробки інформаційної системи захисту інтелектуальної власності на мультимедійні дані (далі – система) доцільно розглядати не лише алгоритмічні механізми (хешування, водяні знаки, часові мітки), а й управлінські та соціально-психологічні компоненти взаємодії з платформами і спільнотами, які безпосередньо впливають на швидкість реагування та повторюваність порушень.

У практиці платформ ключовим інструментом є поєднання процедур «notice-and-takedown» з елементами «notice-and-staydown», що передбачає не лише вилучення конкретної копії, а й запобігання повторній появі ідентичних або близьких за змістом матеріалів за рахунок контент-ідентифікації та фільтрації. Дослідження щодо «notice and staydown» підкреслюють потребу балансування між ефективністю блокування та ризиками надмірного обмеження прав користувачів, а також важливість процесуальної коректності повідомлень і доказів. [1]

З огляду на зростання ролі «приватного порядкування» у сфері авторського права, правила спільнот і технічні засоби модерації фактично стають додатковим рівнем регулювання розміщення та використання контенту. Це означає, що правовласник має діяти одночасно у юридичній площині (наявність прав/ліцензії) та процедурній (правильне проходження механізмів платформи). У системі доцільно реалізувати модуль формування «скарги-пакета» з уніфікованими полями, доказами та історією взаємодії. [2]

Соціально-психологічний вимір реагування проявляється у мотивації користувачів і сприйнятті санкцій. Порушення авторських прав часто підтримується соціальними нормами («так роблять усі»), низькою відчутністю шкоди та переконанням у безкарності. Порівняльні дослідження цифрового піратства демонструють значущість соціальних норм і почуття «обов'язку» (duty) для добровільного дотримання правил. Це відкриває можливість для «м'яких» управлінських інтервенцій: прозорих пояснень, посилань на ліцензійні умови, стимулювання легальних альтернатив і формування довіри. [3]

Разом із тим, прямий тиск у публічній площині може викликати реактивний опір та стимулювати пошук альтернативних каналів поширення. Аналіз практик скарг/позначень (flagging) свідчить, що без чітких доказів і узгоджених дій платформи просте «масове позначення» не гарантує ефективного результату, а інколи може бути контрпродуктивним. Тому система повинна підтримувати доказовість і точність, а не лише кількісні показники активності. [4]

Окремий напрям – комунікаційні кампанії проти піратства, де ефективність залежить від фреймінгу повідомлення, залученості аудиторії, сприйнятого ризику та наявності переконливих доказів (message evidence). Для правовласника це означає потребу у стандартизованих коротких роз'ясненнях (не лише юридичних формулюваннях) та каналах зворотного зв'язку, що знижує ескалацію конфліктів і підвищує добровільне дотримання правил. [5]

З урахуванням зазначеного пропонується інтегрувати у систему: (1) OSINT-моніторинг і пошук збігів (перцептивний хеш, метадані, ідентифікатор водяного знака); (2) управління інцидентами (класифікація, пріоритезація,

таймлайн); (3) комунікацію з платформами (шаблони звернень, журнали відправки, трекінг статусів); (4) взаємодію зі спільнотою (FAQ, довідкові повідомлення, сценарії ескалації); (5) аналітику повторних копій та ефективності втручань. На рис. 1 подано узагальнений цикл, який поєднує технічне виявлення збігів із управлінською логікою реагування та повторним контролем.

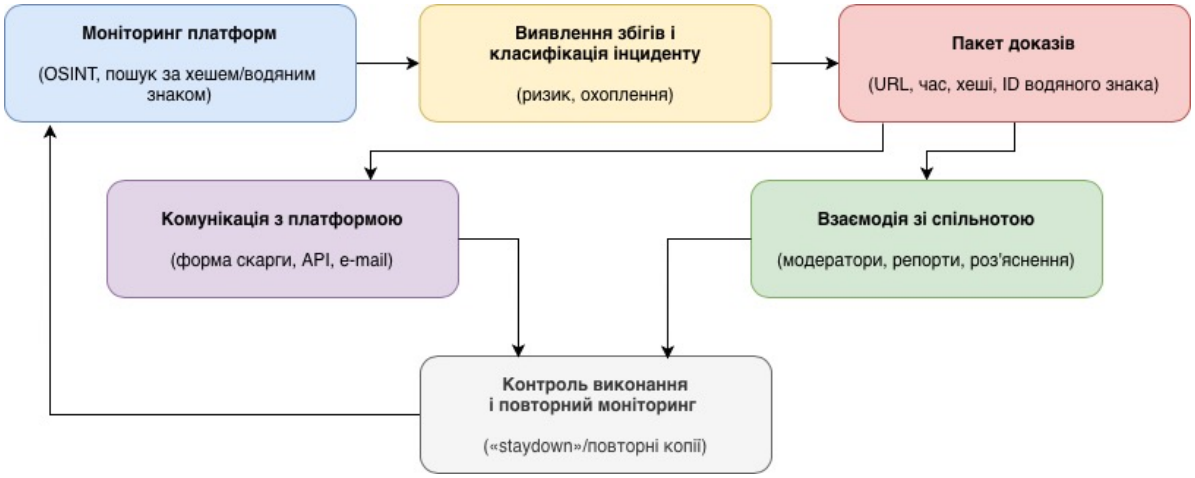

Рис. 1. Комунікаційно-технічний цикл реагування на репости та «дзеркала» контенту.

Нижче наведено узагальнену матрицю ролей/каналів і метрик, яку можна використати як основу «playbook» реагування (табл. 1).

Табл. 1. Узагальнена матриця взаємодії з платформами та спільнотами.

Суб'єкт/роль	Канал взаємодії	Що формує система	Показники ефективності (приклади)
Правовласник	Форма/e-mail/API	Пакет доказів; шаблон звернення	TTR; частка вилучень
Платформа (Trust & Safety)	Кейс-трекинг	Уніфіковані поля; докази; статуси	Час модерації; повтори
Модератори спільнот	Репорти/DM	Коротке пояснення; посилання на ліцензію	Ескалації; видалення
Оператор системи	Дашборд	Пріоритезація; граф копій; звіти	Рецидив; охоплення

Ефективна протидія репостам і «дзеркалам» мультимедійного контенту потребує поєднання технічних механізмів ідентифікації (перцептивні відбитки, водяні знаки, фіксація часу та версій) із керованим процесом взаємодії з платформами. Результативність звернень визначається не кількістю скарг, а якістю доказового пакета, коректністю процедурного маршруту та здатністю підтримувати «staydown»-контроль через повторний моніторинг.

Комунікація зі спільнотами має зменшувати конфліктність і стимулювати добровільне дотримання правил: короткі пояснення, прозорі посилання на ліцензійні умови, готові FAQ і канали зворотного зв'язку знижують реактивний опір та рецидив. Для інформаційної системи це означає інтегрований «playbook» реагування: від автоматизованого виявлення копій і пріоритезації інцидентів — до трекінгу кейсів та оцінювання ефективності комунікаційних стратегій.

Список використаної літератури:

1. Romero-Moreno F. Notice and staydown and social media. International Review of Law, Computers & Technology. 2018. DOI: 10.1080/13600869.2018.1475906.
2. Quintais J.P., De Gregorio G., Magalhães J.C. How platforms govern users 'copyright-protected content. Computer Law & Security Review. 2023;48:105792. DOI: 10.1016/j.clsr.2023.105792.
3. van Rooij B., Fine A., Zhang Y., Wu Y. Comparative Compliance: Digital Piracy, Deterrence, Social Norms, and Duty. Law & Policy. 2017. DOI: 10.1111/lapo.12071.
4. Chipidza W., Yan J. The effectiveness of flagging content: the case of Donald Trump on Twitter. JASIST. 2022;73(11):1641-1658. DOI: 10.1002/asi.24705.
5. Jeong B.K., Yoon T., Khan S.S. Anti-Piracy Educational Deterrence Efforts. JTAER. 2021;16(3):298-319. DOI: 10.3390/jtaer16030021.

Ключові слова: інтелектуальна власність, мультимедійні дані, кіберпростір, контент-модерація, репости, «дзеркала», повідомлення та вилучення, цифрові докази, поведінкові чинники.

Keywords: intellectual property, multimedia data, cyberspace, content moderation, reposts, mirror sites, notice-and-takedown, digital evidence, behavioral factors.

Науковий керівник: к.т.н., доцент Ахмаметьєва Г.В.

ПЛАТФОРМЕНА ЕКОНОМІКА: МОЖЛИВОСТІ ТА ВИКЛИКИ

Маріна Аліна

студентка 1 курсу Факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Платформена економіка — це новий етап розвитку глобального господарства, який змінює класичні уявлення про бізнес, працю і споживання. Її суть полягає у створенні цифрових середовищ, які забезпечують обмін товарами, послугами та інформацією між численними користувачами. Така модель набула поширення завдяки стрімкому розвитку технологій, доступу до Інтернету та поширенню мобільних пристроїв. Сьогодні платформена економіка є не лише частиною цифрової трансформації, а й одним із провідних чинників соціально-економічних змін і перетворюється на ключовий драйвер розвитку глобального господарства [1].

Її вплив охоплює економічні, соціальні та управлінські процеси, змінюючи традиційні моделі організації бізнесу, взаємодії між учасниками ринку та механізми ухвалення рішень. Поширення цифрових платформ стало основою нових механізмів координації, де центральним ресурсом виступають інформація, алгоритми та дані, що формують логіку взаємодії між користувачами [2].

Зростання цифрових екосистем формує сучасні управлінські підходи. Більшість процесів у платформеній економіці здійснюється в режимі реального часу, що потребує від менеджерів високого рівня цифрової компетентності, аналітичних навичок та здатності працювати з великими масивами даних [3].

Управлінська діяльність дедалі більше зосереджується на координації учасників екосистеми, узгодженні їх інтересів та забезпеченні прозорих умов для взаємодії. Таким чином, роль менеджера зміщується від контролю до стратегічного управління взаємозв'язками всередині цифрового середовища.

Окремого значення набуває формування довіри у платформеній моделі бізнесу. Рейтинги, відгуки, алгоритмічні механізми перевірки якості — усе це замінює традиційні інституційні засоби контролю й забезпечує конкурентні переваги платформам, здатним гарантувати стабільність і надійність цифрового середовища. Репутаційний капітал у таких умовах стає стратегічним ресурсом і суттєво впливає на успішність бізнес-моделі.

У соціальному вимірі платформена економіка стимулює формування нових моделей зайнятості та підприємництва. Вона розширює доступ до ринку для малого бізнесу, фрілансерів і фахівців, що працюють дистанційно, створюючи високу гнучкість та можливості участі у глобальних процесах. Водночас такі моделі потребують модернізації системи регулювання, насамперед щодо забезпечення прав працівників та користувачів [4].

Для України розвиток платформеної економіки має стратегічне значення. Активне впровадження цифрових сервісів у державному управлінні, фінансовому секторі, логістиці й освіті свідчить про поступову інтеграцію країни в глобальні цифрові ринки. Платформи забезпечують нові можливості для бізнесу, сприяють економічному зростанню та підвищують ефективність взаємодії між учасниками ринку навіть за умов обмежених ресурсів.

Попри значний потенціал, платформена економіка стикається з низкою викликів. Серед них — концентрація великих масивів даних у технологічних компаній, ризики монополізації та необхідність створення ефективного правового поля, здатного оперативно реагувати на динаміку технологічних змін. Особливої уваги потребують питання кібербезпеки, конфіденційності даних та прозорості алгоритмів, оскільки вони є критично важливими для сталого розвитку галузі.

Перспективи до кінця десятиліття пов'язані з подальшою інтеграцією штучного інтелекту, блокчейну та технологій Інтернету речей, що сприятиме

автоматизації управлінських процесів, оптимізації транзакцій та формуванню нових бізнес-моделей. Психологічні аспекти взаємодії в цифровому середовищі мають допоміжний характер і пов'язані здебільшого зі здатністю користувачів адаптуватися до інформаційних навантажень та підтримувати довіру до цифрових сервісів.

Отже, платформена економіка формує нову архітектуру соціально-економічних відносин, у якій управлінські, технологічні та інституційні чинники взаємодіють комплексно та підсилюють один одного. Успішний розвиток платформних моделей залежить від поєднання технологічних інновацій, ефективного державного регулювання та високої цифрової культури суспільства.

Список використаних джерел

1. Bartels N. Developing network effects for digital platforms in two-sided markets [Електронний ресурс]. URL: https://surl.lu/pxdpbt (дата звернення: 10.11.2025).
2. Digital Platforms and Network Effects // Cornell University Blog [Електронний ресурс]. URL: https://surl.li/fimwba (дата звернення: 10.11.2025).
3. OECD. The impact of digital technologies on well-being [Електронний ресурс]. URL: https://surl.lu/yonlxs (дата звернення: 10.11.2025).
4. Crolic C. Social platform use and psychological well-being // Journal of Consumer Psychology [Електронний ресурс]. URL: https://surl.li/zzhgdn (дата звернення: 10.11.2025).
5. Oluka A. The impact of digital platforms on traditional business and labour markets *Таврійський економічний журнал* [Електронний ресурс]. URL: https://surl.li/upadnw (дата звернення: 10.11.2025).

Ключові слова: платформена економіка; цифрові платформи; управління; цифрова екосистема; дані; бізнес-моделі; цифрова трансформація; штучний інтелект.
Keywords: platform economy; digital platforms; management; digital ecosystem; data; business models; digital transformation; artificial intelligence.

Науковий керівник: к.ю.н. доцент Чанишев Р.І.

НМІ ЯК ЧИННИК ЦИФРОВОЇ ЕВОЛЮЦІЇ УПРАВЛІНСЬКИХ ПРАКТИК

Кочубинська Юлія
студентка 1 курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Технології взаємодії людина–машина (Human–Machine Interaction, HMI) є одним із найдинамічніших напрямів розвитку сучасної науки та бізнесу. Вони формують нову епоху цифрової комунікації, у якій межі між людиною та машиною поступово стираються. Сьогодні такі технології застосовуються у

виробництві, медицині, транспорті, освіті, сфері послуг і навіть у правовій системі. Водночас зростає потреба в адаптації співробітників до роботи в умовах автоматизації, штучного інтелекту (ШІ) та роботизації [1].

HMI змінює не лише технічні процеси, а й соціальні, психологічні та етичні аспекти взаємодії у робочих колективах. Людина стає не просто користувачем, а партнером машини, від якого залежить ефективність прийняття рішень. Тому ключовим завданням сучасного менеджменту є забезпечення гармонійної інтеграції технологій у робоче середовище та створення умов для комфортної адаптації персоналу.

Концепція HMI охоплює різні рівні взаємодії — від інтерфейсів користувача у смартфонах до складних систем керування промисловими роботами. Основна мета полягає в тому, щоб зробити комунікацію між людиною та машиною інтуїтивною, ефективною та безпечною. Сучасні системи HMI базуються на принципах когнітивної ергономіки, аналізі поведінки користувача та машинному навчанню. Це дозволяє створювати інтерфейси, що самонавчаються й адаптуються до індивідуальних особливостей працівників [2].

Інтерактивні системи типу «людина–машина» вже сьогодні реалізовані у таких галузях, як медицина (роботи-хірурги), транспорт (автономні автомобілі), банківська справа (чат-боти і голосові помічники) та промисловість, де HMI використовується як основа для роботизованих систем управління [3; 4].

Технології людина–машина дозволяють суттєво підвищити ефективність роботи підприємств. Вони знижують кількість помилок, прискорюють обмін інформацією, дають змогу приймати рішення на основі даних, а не припущень. Наприклад, у промисловості HMI допомагають контролювати обладнання в реальному часі, у медицині — діагностувати захворювання за допомогою ШІ, а в освіті — створювати персоналізовані програми навчання.

Крім того, HMI сприяє розвитку аналітичного мислення у співробітників. Вони вчаться не лише виконувати команди системи, а й розуміти логіку її роботи. Це формує нову культуру співпраці, де людина й машина діють як частини єдиного інтелектуального середовища.

Окрім цих переваг, важливо усвідомлювати, що HMI створює нові моделі взаємодії, які розмивають межі між традиційними ролями «оператора» та «системи». Сучасна організація має розглядати працівника не як споживача технології, а як активного співтворця інтерфейсу і співучасника процесу. Менеджменту доводиться змінювати підхід: не просто впроваджувати технологію, а моделювати сценарії її використання разом із користувачем, враховуючи фактори довіри, культурні і особистісні відмінності. Це відкриває

потенціал не лише для підвищення продуктивності, а й для створення нових цінностей у організації.

У майбутньому інтеграція HMI з технологіями доповненої й віртуальної реальності (AR/VR), біоінтерфейсами та нейромережами створить середовище, в якому людина зможе взаємодіяти з машинами на рівні думки та інтуїції. [5]

Проте головним фактором успіху залишатиметься етична відповідальність: машини не повинні замінювати людський вибір чи підмінювати моральні рішення. Технології мають підтримувати людину та її цінності, а не їх заміщати.

Попри очевидні переваги, масове впровадження HMI породжує низку проблем. Найсерйознішими є страх втрати роботи через автоматизацію, зниження мотивації, техностpес і психологічна втома від постійного контакту з машинами. Співробітники часто відчувають тривогу через невпевненість у своїй компетентності, особливо коли технології змінюються швидше, ніж вони встигають навчитися.

Крім того, актуальними є питання етики та приватності. Використання біометричних даних, голосових команд і алгоритмів розпізнавання облич вимагає чітких правил зберігання інформації. Менеджери мають забезпечити баланс між ефективністю і безпекою, між автоматизацією та людською участю.

Процес адаптації до HMI включає технічне, психологічне й організаційне навчання. Найефективнішою стратегією є поступове впровадження нововведень, коли працівники мають можливість ознайомитися з функціоналом системи, пройти тренінги та побачити її переваги. Важливу роль відіграє внутрішня комунікація: працівники мають бачити, що технології не замінюють їх, а допомагають виконувати роботу швидше та якісніше.

Адаптація також пов’язана із розвитком емоційного інтелекту. Людина, яка розуміє власні емоції та вміє контролювати стрес, легше приймає нововведення. Тому сучасні компанії включають у програми навчання елементи психологічної підтримки й командного коучингу.

Технології HMI змінюють структуру економіки. З’являються нові професії — оператори роботизованих систем, аналітики даних, фахівці з цифрової етики. Водночас частина рутинних робіт зникає, а це потребує державної підтримки перекваліфікації працівників. Для країн, що розвиваються, зокрема України, важливо створити програми підготовки кадрів для цифрової економіки.

На рівні організацій HMI стає основою управління знаннями. Дані, зібрані машинами, перетворюються на управлінські рішення. Це вимагає від керівників нових навичок — стратегічного мислення, аналітичних здібностей і розуміння принципів роботи штучного інтелекту.

У найближчі роки HMI інтегруватиметься з технологіями доповненої та віртуальної реальності (AR/VR), біоінтерфейсами та нейромережами. Людина зможе керувати машинами силою думки, а інтерфейси стануть максимально природними.

Це відкриває перспективи для медицини, освіти, права та державного управління.

Разом із тим, ключовим фактором залишатиметься етична відповідальність. Машини не повинні порушувати права людини чи підмінювати моральні рішення. Тому роль людини у взаємодії з технологіями залишатиметься центральною.

Технології взаємодії людина–машина — це не лише інструмент автоматизації, а й нова модель співпраці. Вони створюють умови для підвищення ефективності праці, але водночас вимагають переосмислення ролі людини в системі. Успішна адаптація співробітників залежить від поєднання технічного навчання, психологічної підтримки та етичного контролю. Лише гармонійна взаємодія між людиною і машиною забезпечить стабільний розвиток суспільства в умовах цифрової епохи.

Список використаних джерел

1. [Human-Machine Interaction – an overview [Електронний ресурс]. URL: https://www.sciencedirect.com/topics/engineering/human-machine-interaction (дата звернення: 10.11.2025).
2. What is HMI? Human Machine Interface (HMI) – Inductive Automation [Електронний ресурс]. URL: https://inductiveautomation.com/resources/article/what-is-hmi (дата звернення: 10.11.2025).
3. Solanes J.E. “Advances in Human–Machine Interaction, Artificial Intelligence and Robotics” [Електронний ресурс]. URL: https://www.mdpi.com/2079-9292/13/19/3856 (дата звернення: 10.11.2025).
4. Gao Z. “Better interaction experience: human-machine interface for soft robotic systems” [Електронний ресурс]. URL: https://www.oaepublish.com/articles/ir.2025.27 (дата звернення: 10.11.2025).
5. Mourtzis D., Angelopoulos J., Panopoulos N. “The Future of the Human–Machine Interface (HMI) in Society 5.0” [Електронний ресурс]. URL: https://www.researchgate.net/publication/370865068_The_Future_of_the_Human-Machine_Interface_HMI_in_Society_5.0 (дата звернення: 10.11.2025).

Ключові слова: HMI; технології людина–машина; цифрове регулювання; автоматизація праці; адаптація персоналу; цифрова трансформація; штучний інтелект
Keywords: HMI; human–machine technologies; digital regulation; labor automation; personnel adaptation; digital transformation; artificial intelligence.

Науковий керівник: к.ю.н. доцент Чанишев Р.І.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОДУКТИВНОСТІ ДЕКЛАРАТИВНОГО ТА ІМПЕРАТИВНОГО ПІДХОДІВ ДО ПОБУДОВИ КОРИСТУВАЦЬКИХ ІНТЕРФЕЙСІВ МОБІЛЬНИХ ЗАСТОСУНКІВ

Земан Артур

студент факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

Індустрія розробки мобільних застосунків переживає фундаментальний зсув у підходах до створення користувацьких інтерфейсів. Протягом багатьох років домінував імперативний підхід, представлений в Android традиційною системою View. Однак останнім часом все більшої популярності набуває декларативна парадигма, яскравим представником якої є фреймворк Jetpack Compose від Google. Великі компанії вже здійснили міграцію на Jetpack Compose, проте бракує комплексних академічних досліджень, які б надавали кількісну оцінку продуктивності декларативного підходу в порівнянні з імперативним з використанням сучасних інструментів для бенчмаркінгу.

Метою дослідження є порівняльний аналіз продуктивності мобільних застосунків при використанні декларативного та імперативного підходів до побудови користувацьких інтерфейсів та розробка практичних рекомендацій для розробників. Для досягнення мети необхідно було проаналізувати теоретичні основи та архітектурні відмінності підходів, розробити методологію експериментального дослідження, провести тестування продуктивності за ключовими показниками та здійснити статистичний аналіз отриманих даних.

Методологія дослідження базується на комплексному використанні сучасних спеціалізованих інструментів профілювання та бенчмаркінгу. Для вимірювання продуктивності застосовувалася бібліотека Jetpack Macrobenchmark [1], Android Studio Profiler для профілювання системних ресурсів, Perfetto для системного трасування та JankStats API для моніторингу плавності інтерфейсу. Визначено чотири критичні категорії вимірювань: метрики продуктивності під час виконання, метрики пам'яті, метрики збірки та метрики енергоспоживання. Критичним аспектом методології стало використання виключно релізних збірок із увімкненою оптимізацією, оскільки Debug-збірки демонструють продуктивність понад удвічі повільнішу [2].

Експериментальне дослідження охопило аналіз реальних промислових впроваджень. Команда OkCredit провела дослідження на реальних користувачах, де екран на основі Compose без попередньої компіляції завантажувався у два з половиною рази довше порівняно з традиційною системою [3]. Водночас після попередньої компіляції компонентів спостерігалося значне скорочення заморожених кадрів та суттєве покращення часу завантаження завдяки механізму попередньої компіляції Android Runtime [3].

Офіційна документація Android надає рекомендації щодо порівняння метрик продуктивності [4]. Аналіз зразкового додатку Sunflower показав, що при додаванні Compose розмір пакету збільшується приблизно на третину. Проте реальний приклад додатку Tivi демонструє, що після повної міграції розмір пакету скоротився майже вдвічі, а час збірки покращився приблизно на третину [5].

Дослідження команди Premise Engineering виявило критичну важливість конфігурації збірки [2]. Збірки з вимкненою оптимізацією виконувалися понад удвічі довше, що підкреслює необхідність тестування виключно в релізному режимі [6]. Базові профіли виявилися критичним фактором для досягнення конкурентної продуктивності, покращуючи швидкість виконання коду приблизно на третину від першого запуску [7].

Порівняння компонентів списків LazyColumn та RecyclerView показало, що холодний запуск значно повільніший з Compose, проте продуктивність прокручування практично ідентична [8]. Дослідження оптимізації управління станом виявило можливість значного скорочення споживання пам'яті при використанні правильних патернів [9].

Статистичний аналіз виявив два різні режими продуктивності Compose: початковий без належної конфігурації з деградацією продуктивності та оптимізований з попередньою компіляцією, що досягає найкращих показників. Кореляційний аналіз демонструє стабільну тенденцію поліпшення з кожним релізом.

На основі отриманих результатів сформульовано практичні рекомендації. Для нових проєктів рекомендовано використання Jetpack Compose завдяки прискоренню циклу розробки та скороченню обсягу коду. Для існуючих застосунків доцільна поступова міграція. Критично важливим є увімкнення повної оптимізації коду, створення базових профілів та дотримання принципів стабільності параметрів композиційних функцій.

Результати дослідження підтверджують, що декларативний підхід досяг паритету з імперативним у більшості метрик продуктивності та демонструє переваги у критичних сценаріях після належної оптимізації. Розроблена методологія може використовуватися для оцінки продуктивності інших UI-фреймворків.

Список використаної літератури:

1. Android Developers. Write a Macrobenchmark. URL: https://developer.android.com/topic/performance/benchmarking/macrobenchmark-overview (дата звернення: 10.11.2025).
2. Shelor W. Measuring Render Performance with Jetpack Compose / Will Shelor // Premise Engineering Blog. 2021. October 26. URL: https://engineering.premise.com/measuring-render-performance-with-jetpack-compose-c0bf5814933

3. Arora P. Comparing Jetpack Compose performance with XML / Pratham Arora // Medium — OkCredit. 2022. August 9. URL: https://medium.com/okcredit/comparing-jetpack-compose-performance-with-xml-9462a1282c6b
4. Android Developers. Compare Compose and View metrics. URL: https://developer.android.com/develop/ui/compose/migrate/compare-metrics (дата звернення: 10.11.2025).
5. Banes C. Jetpack Compose — Before and after / Chris Banes // Medium — Android Developers. 2021. July 7. URL: https://medium.com/androiddevelopers/jetpack-compose-before-and-after-8b43ba0b7d4f
6. Trengrove B. Why should you always test Compose performance in release? / Ben Trengrove // Medium — Android Developers. 2022. June 8. URL: https://medium.com/androiddevelopers/why-should-you-always-test-compose-performance-in-release-4168dd0f2c71
7. Semenova K., Ravikumar R., Craik C. Improving App Performance with Baseline Profiles // Android Developers Blog. 2022. January 27. URL: https://android-developers.googleblog.com/2022/01/improving-app-performance-with-baseline.html
8. MarDSoul. RecyclerView vs LazyColumn / MarDSoul // DEV Community. 2024. July 25. URL: https://dev.to/mardsoul/recyclerview-vs-lazycolumn-5g6g
9. Patil S. Benchmark Insights: Direct State Propagation vs. Lambda-based State in Jetpack Compose / Shreyas Patil // Personal Blog. 2024. November 19. URL: https://blog.shreyaspatil.dev/benchmark-insights-direct-state-propagation-vs-lambda-based-state-in-jetpack-compose

Ключові слова: Jetpack Compose, Android Views, декларативний підхід, продуктивність, бенчмаркінг, рекомпозиція, оптимізація.
Keywords: Jetpack Compose, Android Views, declarative approach, performance, benchmarking, recomposition, optimization.

COMPETITION AND MARKETS AUTHORITY (CMA): УПРАВЛІННЯ КОНКУРЕНЦІЄЮ В ЕПОХУ ЦИФРОВИХ РИНКІВ

Власюк Олександра
студентка 1 курсу факультету судового та міжнародного права Національного університету «Одеська юридична академія»

Competition and Markets Authority (CMA) є ключовим антимонопольним регулятором Великої Британії — він відповідає за підтримання добросовісної конкуренції, захист споживачів і забезпечення прозорості ринкових процесів. З моменту свого повноцінного запуску у 2014 році CMA відіграє визначну роль у формуванні регуляторної політики, однак саме цифрова трансформація суттєво розширила її повноваження та ускладнила управлінські задачі. У контексті домінування великих технологічних платформ, змін у поведінці споживачів та появі нових форм цифрових бізнес-моделей CMA має адаптувати традиційні механізми конкурентної політики до нових умов цифрової економіки.

Цифрова трансформація супроводжується швидким розвитком платформенної економіки, в якій ринкова влада дедалі частіше концентрується не у класичних монополістів галузей, а у глобальних цифрових екосистемах. Це створює специфічні виклики для регулятора: класичні підходи до оцінювання конкуренції — аналіз ринкових часток, структури галузі чи ціноутворення — стають недостатніми. Прикладом є роль даних як стратегічного ресурсу, мережеві ефекти, висока швидкість масштабування цифрових сервісів або алгоритмічне управління цінами [1].

Одним із центральних напрямів діяльності CMA у цифрову епоху є регулювання поведінки великих технологічних компаній, які отримують так званий статус стратегічного ринкового суб'єкта (Strategic Market Status, SMS). У відповідь на зростання концентрації цифрової влади CMA створила підрозділ Digital Markets Unit (DMU). Цей підрозділ має розробляти правила й стандарти для великих цифрових платформ — у сферах онлайн-пошуку, соціальних мереж, електронної комерції та цифрової реклами [3-2].

Важливою складовою діяльності CMA є моніторинг впливу штучного інтелекту (ШІ) на конкурентну динаміку ринків. Алгоритмічне ціноутворення, автоматизовані системи прогнозування попиту, персоналізовані рекламні моделі та рекомендаційні платформи суттєво змінюють поведінку учасників. Існує ризик, що алгоритми різних компаній, навіть без прямої змови, можуть «узгоджувати» стратегії, створюючи приховані ознаки антиконкурентності. CMA досліджує ці процеси та аналізує питання відповідальності за рішення, ухвалені автоматизованими системами [2-3].

Окрему увагу CMA приділяє міжнародній співпраці, оскільки великі цифрові платформи працюють одночасно в багатьох країнах, а потенційні зловживання ринковою владою або антиконкурентна поведінка майже завжди мають транскордонний характер. Після виходу Великої Британії з ЄС важливим кроком стало укладення угоди про співробітництво у сфері конкуренції між ЄС та Великою Британією, яка передбачає обмін інформацією, координацію розслідувань і узгодження підходів до аналізу концентрацій, картелів та зловживання домінуючим становищем. Це дозволяє CMA і Єврокомісії паралельно розглядати одні й ті самі глобальні угоди щодо злиття чи поведінки великих платформ, зменшуючи ризик суперечливих рішень і прогалин у нагляді.

Крім взаємодії з ЄС, CMA бере участь у роботі Організації економічного співробітництва та розвитку (OECD), Міжнародної мережі з питань конкуренції (ICN), а також у спеціалізованих робочих групах і круглих столах ООН (UNCTAD), де узгоджуються підходи до розслідування глобальних злиттів, картелів і цифрових ринків. У цих форматах CMA обмінюється досвідом з Федеральною торговою комісією США (FTC), Єврокомісією та іншими потужними відомствами, відпрацьовуючи механізми координації в конкретних

справах, включно з хмарними сервісами, онлайн-рекламою та ШІ-платформами. Така співпраця дає змогу узгоджувати часові рамки розгляду справ, мінімізувати регуляторні прогалини в транскордонних угодах і формувати більш послідовну глобальну практику застосування конкурентного права. [4]

У сфері доступу до даних СМА виступає арбітром, що контролює прозорість алгоритмів, недискримінаційні умови для бізнес-користувачів та використання даних великими платформами. Концентрація великих обсягів інформації в окремих цифрових гравців формує бар'єри входу для інших компаній, що потребує регуляторного реагування [5].

Ще одним управлінським напрямом СМА є контроль за злиттями та поглинаннями у цифровому секторі. На відміну від традиційних ринків, цифрові гіганти часто купують стартапи для запобігання появі майбутніх конкурентів («killer acquisitions»). СМА аналізує не лише поточний стан ринку, а й потенційний довгостроковий вплив технологічних інновацій.

Управлінські аспекти діяльності СМА включають розвиток цифрової експертизи, адаптацію внутрішніх процедур, використання економічного моделювання, аналіз поведінкових моделей та аудит алгоритмічних систем. Це потребує мультидисциплінарних команд та швидкої реакції на появу нових цифрових технологій.

Особливу роль СМА відіграє у захисті споживачів у цифровому середовищі. Йдеться про боротьбу з маніпулятивними інтерфейсами («dark patterns»), некоректними підписками, оманливою рекламою та непрозорими умовами цифрових сервісів.

Після Brexit СМА отримала повну автономію у сфері цифрових ринків, формуючи власну модель регулювання. Велика Британія створює нормативну базу, здатну реагувати на виклики ШІ, блокчейн-платформ, автоматизованої торгівлі та нових типів цифрових посередників.

Таким чином, роль СМА у цифровій економіці поступово перетворюється на стратегічний механізм забезпечення збалансованого розвитку ринків, які швидко змінюються під впливом інноваційних технологій. Завдяки поєднанню аналітичних інструментів, регуляторних повноважень і цифрової експертизи регулятор створює умови, що одночасно підтримують інноваційність бізнесу та запобігають посиленню ринкової концентрації, забезпечуючи стабільність і прозорість цифрового середовища.

Регуляторна діяльність СМА знижує ризики монополізації, сприяє відкритості ринків, стимулює появу нових бізнес-моделей і підвищує рівень захисту споживачів у цифровому середовищі. Створюючи чіткі правила поведінки для великих платформ, СМА гарантує, що розвиток нових технологій відбуватиметься у рамках справедливих та прозорих механізмів ринкової взаємодії. У більш широкому контексті це забезпечує підвищення

довіри до цифрових послуг, формування конкурентних стимулів для інновацій та зміцнення позицій Великої Британії як одного з лідерів цифрової економіки.

Список використаних джерел

1. Competition and Markets Authority. How the UK's digital markets competition regime works. 10.02.2025. URL: https://www.gov.uk/guidance/how-the-uks-digital-markets-competition-regime-works (дата звернення: 06.11.2025).
2. Egerton-Doyle V., Hunter J. The UK's New Digital Markets Regime: Unfettered Discretion and Power for the CMA. Linklaters Competition Blog. 07.10.2024. URL: https://legalblogs.wolterskluwer.com/competition-blog/the-uks-new-digital-markets-regime-unfettered-discretion-and-power-for-the-cma (дата звернення: 06.11.2025).
3. Competition and Markets Authority. CMA Digital – Data and Technology Insight blog. 08.11.2024. URL: https://surl.li/dqlppt (дата звернення: 06.11.2025).
4. Competition and Markets Authority. The CMA's Digital Markets Strategy. July 2019. URL: https://surl.li/pobbge (дата звернення: 06.11.2025).
5. Competition and Markets Authority. Consultation on new digital markets competition guidance. 19.12.2024. URL: https://connect.cma.gov.uk/cma-new-digital-markets-regime (дата звернення: 06.11.2025).

Ключові слова: конкуренція, цифрові ринки, платформи, антимонопольний регулятор, цифрова трансформація
Keywords: competition, digital markets, platforms, antitrust regulator, digital transformation.

Науковий керівник: к.ю.н. доцент Чанишев Р.І.

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Задерейко Олександр

доцент, кандидат технічних наук, доцент кафедри інформаційних технологій факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Іванов Володимир

студентка 4-го курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

У сучасному світі інформація і цифрові сервіси [1] стали фундаментальною інфраструктурою суспільного життя. Шкала використання інформаційних технологій у державному управлінні, енергетиці, банківській сфері, медицині та освіті вимагає надійних правових механізмів, які б забезпечували не лише технічний захист, а й відповідальність, координацію та прозорість. Поняття кібербезпеки розглядається сьогодні як комплексна категорія, що включає правові, організаційні, технічні та соціальні складові. Тенденції останнього десятиліття свідчать про те, що масштабні кібератаки отримали стратегічний характер: вони можуть впливати на економічну стабільність, критичні системи життєзабезпечення і навіть на результати політичних процесів. Для держави таке явище стає питанням не лише безпеки, а й суверенітету [2].

Нормативно-правове поле [3], яке регулює відносини у сфері кібербезпеки, має дві взаємопов'язані цілі. Перша полягає у створенні умов для превентивного захисту, що передбачає впровадження стандартів, сертифікацію засобів захисту, встановлення обов'язків щодо оцінки ризиків та реалізації заходів захисту у критичних і некритичних інформаційних системах. Друга мета — забезпечення дієвих механізмів реагування та правозастосування у випадку інцидентів. Законодавство має бути спроможним не лише визначити відповідальність, але й забезпечити оперативну міжнародну співпрацю у сфері розслідування кіберзлочинів, екстрадицію, обмін інформацією та координацію технічної допомоги.

В Україні правове регулювання в цій сфері базується на низці ключових нормативних актів, серед яких центральне місце займає Закон України «Про основні засади забезпечення кібербезпеки України». Цей акт визначає понятійний апарат, статус суб'єктів системи кібербезпеки, базові принципи державної політики, а також інструментарій захисту критичної інформаційної

інфраструктури. У законі закріплено підходи до створення національних центрів реагування, визначення ролей державних установ та встановлення механізмів взаємодії з приватними операторами. Паралельно з національними актами, правове поле доповнюється правилами, що стосуються захисту інформації в інформаційно-телекомунікаційних системах, регулюванням обігу персональних даних та правами громадян у цифровому просторі.

Законодавство про захист персональних даних має спеціальне значення у загальній системі кібербезпеки. Воно формує правові гарантії приватності, є інструментом захисту фізичних осіб від безпідставного збору, обробки або передачі інформації, яка може завдати шкоди. У рамках цифрової взаємодії між громадянами, бізнесом і державою правила обробки персональних даних визначаються прозорі процедури надання згоди, термінів зберігання, механізмів доступу до інформації та прав на видалення. Гармонізація національного законодавства з міжнародними нормами, зокрема з правилами ЄС, сприяє підвищенню довіри та інтеграції на транснаціональному рівні.

Міжнародно-правовий контекст відіграє ключову роль у формуванні ефективних механізмів протидії кіберзагрозам [4]. Асамблеї і договори, ініціативи у межах Організації Об’єднаних Націй, рамкові документи Ради Європи та положення НАТО створюють базис для узгодження підходів. Конвенція Ради Європи про кіберзлочинність встановлює стандарти криміналізації деяких дій у кіберпросторі і механізми міжнародної співпраці у справах розслідування злочинів. Міжнародні стандарти також формують практики ведення цифрової криміналістики, обміну інформацією про загрози та спільного реагування на інциденти. Для України важливим є не лише приєднання до міжнародних угод, а й активна участь у розробці процедур співпраці, які враховують специфіку національного інформаційного простору.

Сучасні технологічні тенденції висувають на перший план такі питання, як захист систем, що використовують штучний інтелект [5]. Моделі штучного інтелекту можуть застосовуватися для виявлення загроз, проте водночас вони стають об’єктом атак: атаки на дані навчання, маніпуляції вхідними даними або створення шкідливих автоматизованих сценаріїв. Deepfake - технології, які дозволяють створювати реалістичні підроблені аудіо і відео, ставлять під сумнів довіру до цифрових джерел інформації і вимагають відповідних юридичних інструментів для захисту прав і репутації громадян та інституцій. Законодавство має передбачати відповідальність за створення і поширення матеріалів, що використовуються для введення в оману, однак при цьому не повинно обмежувати свободу вираження поглядів.

Критична інформаційна інфраструктура є особливо вразливою ланкою держави. Порушення роботи енергетичних мереж, систем водопостачання, транспортних вузлів або платіжних систем може мати безпосередні гуманітарні та економічні наслідки. Тому нормативно-правові засади мають

передбачати спеціальні режими захисту таких систем, вимоги до операторів критичної інфраструктури щодо інвестицій у кіберзахист, регулярних аудитів та моделювання сценаріїв атак. Законодавчі норми повинні стимулювати впровадження відновлювальних планів та резервних механізмів для забезпечення безперебійності роботи у кризових ситуаціях.

Інституційна система кібербезпеки [6] передбачає чіткий розподіл обов'язків між державними органами і створення національних центрів, які забезпечують моніторинг, виявлення та реагування на кіберінциденти. Координація дій між різними відомствами, оперативний обмін інформацією з приватним сектором, а також створення механізмів довірчого обміну даними є ключовими умовами ефективності. Одночасно важливим є розвиток людського капіталу: підготовка експертів, створення навчальних програм у вищих навчальних закладах і підвищення кваліфікації працівників держсектору.

Правозастосування у випадках кіберзлочинів має свою специфіку. Слід зазначити, що цифрові докази потребують особливої процедури вилучення, збереження та аналізу. Доказова база у кіберсправах часто має транскордонний характер, що ускладнює оперативність розслідувань без налагоджених міжнародних каналів співпраці. Тому законодавство повинно забезпечувати як внутрішні механізми для ефективного розслідування, так і правову базу для міжнародної допомоги. Крім того, важливою є роль превентивних заходів: розроблення нормативів розробки безпечного програмного забезпечення, впровадження практик захисту на етапі життєвого циклу продукту та стимулювання прозорості у ланцюгах поставок цифрових рішень.

Особливу увагу слід приділяти питанням балансу між забезпеченням безпеки і захистом прав людини. Державні інструменти моніторингу та контролю інформаційних потоків можуть бути ефективними у виявленні загроз, але без належних правових гарантій вони ризикують стати механізмом утиску свободи слова та порушення приватності. Конституційні норми, міжнародні цивільні стандарти і практика Європейського суду з прав людини повинні лягти в основу будь-яких оперативних заходів, спрямованих на захист у кіберпросторі.

Розвиток цифрової економіки [7] вимагає стимулювання інновацій при одночасному забезпеченні захисту споживачів та інтересів національної безпеки. Законодавчі ініціативи повинні створювати прозорі умови для розвитку стартапів, захищати інтелектуальну власність і забезпечувати стандарти кібербезпеки, які не стануть надмірним бар'єром для входу на ринок. Регулятор має враховувати технологічну нейтральність і надавати можливості для добровільної сертифікації та інструментів самоорганізації у галузі.

На завершення, нормативно-правові засади кібербезпеки та захисту інформації вимагають системного підходу, який поєднує законодавчу чіткість, розвиток інституційних механізмів та інвестиції у людський капітал. Тільки при поєднанні цих елементів держава може створити стійку систему, здатну протистояти сучасним загрозам і забезпечити безпечний розвиток цифрового суспільства. У майбутньому важливо фокусуватися на адаптивності правових норм, міжнародній співпраці та інклюзивних підходах, що дозволять поєднати безпеку, права людини і економічний розвиток.

Список використаних джерел:

1. Нікітін, Ю. О., Кульчицький, О. І. Цифрова парадигма як основа визначень: цифровий бізнес, цифрове підприємство, цифрова трансформація. Маркетинг і цифрові технології, 3(4), 2019, С. 77-87.
2. Задерейко О.В., Троянський О.В., Чанишев Р.І., Дика А.І. Концептуальні основи захисту інформаційного суверенітету України : монографія / О.В. Задерейко, О.В. Троянський, Р.І. Чанишев, А.І. Дика. Одеса : Фенікс, 2022. 220 с. ISBN 978-966-928-812-7. URL: https://hdl.handle.net/11300/22733.
3. Корж-Усенко, Л., Рибалко, П. Нормативно-правові засади розвитку вищої освіти в україні в умовах євроінтеграції. Фізико-математична освіта, 29(3), 2021, С. 74–80. DOI: https://doi.org/10.31110/2413-1571-2021-029-3-012/.
4. Ґеник, Микола Антонович. "Методологічні проблеми дефініції термінів «кібербезпека» і «кіберзагроза»." (2025). URL: https://lib-old.pnu.edu.ua/handle/123456789/23115/.
5. Баранов, О. А. (2023). Визначення терміну “штучний інтелект”. Інформація і право, (1 (44)), 32-49. URL: http://il.ippi.org.ua/article/view/287537/281385/.
6. САМОТУГА, А. (2022). Організаційно-інституційне забезпечення інформаційної безпеки України. Науковий вісник Дніпропетровського державного університету внутрішніх, 195. URL: https://lnk.ua/R4aMRyq4J/.
7. Закусило, В., Гавловська, Н., & Власюк, І. (2025). Цифрова економіка та її вплив на управління підприємствами. Рекомендовано до друку науково-технічною радою Хмельницького національного університету, протокол № 11 від 24.12. 2024, 94. URL: https://lnk.ua/Men0bLLNg/.

Ключові слова: кібербезпека; захист інформації; нормативно-правове регулювання; критична інформаційна інфраструктура; кіберзлочинність; захист персональних даних; міжнародне право; штучний інтелект; цифрові докази.

Keywords: cybersecurity; information protection; legal regulation; critical information infrastructure; cybercrime; personal data protection; international law; artificial intelligence; digital evidence.

АНАЛІЗ МЕТОДІВ ВИЛУЧЕННЯ КЛЮЧОВОЇ ІНФОРМАЦІЇ З ЮРИДИЧНИХ ТЕКСТІВ

Гура Володимир

доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Курчук Роман

студент 2-го курсу магістратури факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Обсяги юридичних документів зростають щодня, ускладнюючи швидке виділення ключової інформації, до якої належать учасники справи, застосовані норми права, факти, винесене рішення, мотиви та санкції. Дослідження присвячене методам автоматичного витягування такої інформації з тексту. Проаналізовано багато наукових публікацій з метою виявлення ефективних підходів. Експериментальна перевірка проведена на більш ніж 500 судових рішеннях українською мовою з ЄДРСР трьома методами. Найкращий результат показав метод доповнення контексту нормативними актами використанням пошуку відповідної статті в законодавчій базі з подальшим її використанням для інтерпретації судового тексту. Якість витягування сягнула 89%. Робота підкреслює практичну цінність інструментів для юристів, але вказує на потребу розширення україномовних анотованих наборів даних.

Цифровізація правосуддя в Україні досягла критичного рівня, Єдиний державний реєстр судових рішень (ЄДРСР) містить понад 15 мільйонів документів станом на 2025 рік, з щоденним приростом близько 3–5 тисяч [1]. Ручний аналіз одного рішення займає в середньому 20–40 хвилин, що призводить до перенавантаження суддів, адвокатів та їх співробітників. За даними Мін'юсту України (2024), понад 60% часу юристів витрачається на пошук фактів у текстах, а не на правовий аналіз [2]. Автоматизація цього процесу є не лише питанням ефективності, але й доступності правосуддя, скорочення часу аналізу, за міжнародними аналогами. Вона дозволить прискорити розгляд справ, зменшити судові черги та підвищити якість рішень. У країнах ЄС, наприклад в Естонії та Нідерландах, подібні системи вже інтегровані в судові платформи, скорочуючи час обробки на 50–60% [3]. В Україні, попри наявність відкритих даних, бракує інструментів для автоматичного витягування ключової інформації українською мовою – це створює технологічний розрив.

Ключова інформація – це основні факти, які визначають сутність документа та потрібні для прийняття юридичних рішень. За міжнародними стандартами Legal General Language Understanding Evaluation (LexGLUE) – це

бенчмарк-набір даних для оцінки моделей обробки природної мови Natural Language Processing (NLP) – це обробка природної мови, галузь штучного інтелекту (ШІ), що займається взаємодією комп'ютерів із людською мовою (текстом або усною мовою). Ключова інформація охоплює учасників справи (позивач, відповідач, суддя, свідки) через пошук імен та ролей [4, 5], застосовані норми права (статті законів чи кодексів) через виявлення посилань [6, 7], факти та обставини (дати, місця, події, суми збитків) через виділення подій та зв'язків [8], винесене рішення (визнання вини, задоволення позову, штраф) через визначення результату справи [9], мотиви та аргументи (правові обґрунтування, посилання на практику) через виділення головних тез [10, 11], а також санкції та наслідки (розмір штрафу, термін покарання) через пошук числових даних [12]. Усе це формує чіткий профіль справи, який дозволяє оцінити документ за кілька хвилин. У судових рішеннях України ці дані розкидані по тексту на 5–50 сторінок з різними формулюваннями, що суттєво ускладнює ручний пошук [13].

Цифровізація правової системи України супроводжується експоненційним зростанням обсягів судових рішень та законодавчих актів. Щоденно реєструються тисячі документів, аналіз яких вимагає від юристів значних часових витрат на пошук імен сторін, дат, норм права. Автоматизація цього процесу здатна скоротити час обробки з годин до секунд, зменшити помилки та підвищити доступність правосуддя. За кордоном аналогічні системи вже скорочують час аналізу на 40–60% [10, 11]. В Україні ЄДРСР містить відкриту базу рішень, однак спеціалізованих інструментів для їхньої автоматичної обробки бракує.

Метою дослідження є систематизація сучасних методів, їх апробація на україномовних текстах та формулювання рекомендацій щодо впровадження в судову та адвокатську практику.

Розвиток методів пройшов від простих правил до складних моделей штучного інтелекту. На початку використовували шаблони та словники, наприклад, пошук «ТОВ» як назви компанії чи «ст. 190» як посилання на закон. Такий підхід швидкий, але не витримує варіацій у формулюваннях і дає точність нижче 70% [4].

Далі з'явилися моделі, які навчаються на прикладах. Серед них Bidirectional Encoder Representations from Transformers (BERT) – це нейронна мережа, що читає текст у двох напрямках і враховує контекст. У договорах про злиття вона досягла 85% точності при пошуку сутностей [4]. Подібні результати отримано для судових рішень Індії [5].

Для оцінки ефективності методів автоматичного витягування інформації, з юридичних текстів, створено LexGLUE – набір тестів англійською

мовою для юридичних завдань, пошук імен, класифікація договорів, визначення результату справи [9]. Моделі з механізмом уваги перевершують старі методи на 15–20% у довгих текстах [15, 16].

Класичні моделі **Conditional Random Fields** (CRF) – це **статистична модель для послідовного розпізнавання** (тексту, тегів, сутностей), добре працюють з послідовністю слів і досягли 92% показників при пошуку цитат [6]. Сучасний підхід Retrieval-Augmented Generation (RAG) це ШІ, який не просто "вигадує" відповідь, а шукає її в реальних документах, а потім генерує текст на основі знайденого, це дозволяє шукати потрібні статті в законодавчій базі з подальшим її використанням для пояснення судового тексту. Такий підхід підвищив якість на 18% у текстах португальською мовою [9].

Для мов, відмінних від англійської, розроблено спеціалізовані набори даних. Наприклад, Labor Lex – це анотований датасет португальською мовою, що містить судові рішення та трудові контракти. Він дозволяє навчати моделі витягувати сутності (учасники, норми, факти) та зв'язки між ними з точністю до 85% [14]. Аналогічний підхід застосовано до текстів про COVID-19. Дані для витягування претензій та відповідних норм права забезпечують 80% точності підходу [15]. Попереднє структурування візуально багатих документів (PDF) з виділенням заголовків, абзаців та таблиць підвищує якість витягування на 12% [16], а врахування ієрархії документа – на 15% при узагальненні змісту [10]. Польська, як і українська, має складні закінчення слів. Для польських текстів використовують Rapid Automatic Keyword Extraction (RAKE) – швидкий пошук ключових фраз без навчання, з урахуванням стоп-слів (наприклад, для тендерів), з точністю 70–80% [17]. Статистичні методи на основі груп слів з попереднім спрощенням форм слів (приведення до основи за допомогою Snowball – це фреймворк для створення алгоритмів стемінгу (зведення слів до основи) різними мовами) застосовують для визначення типу справи [18]. Комбіновані моделі ШІ, наприклад Bidirectional Long Short-Term Memory + Conditional Random Field (BiLSTM-CRF) – це ШІ, який читає речення в обидва боки і розумно ставить мітки словам, враховуючи сусідів, з урахуванням нечіткої логіки, дозволяють знаходити неоднозначні терміни та метафори в контрактах, підвищуючи точність на 10–15% [19]. Пошук на основі словників права (онтології) використовують для приховування імен та класифікації [20]. Польська версія BERT добре аналізує законодавчу базу парламенту, з точністю 80–90% [21]. Ці приклади показують, що комбіновані підходи ефективні для слов'янських мов.

У медицині (PubMed, MIMIC-III) пошук на основі графів знань (з медичними словниками UMLS) виділяє симптоми, діагнози, ліки з записів, з точністю 88–92%. Можна адаптувати для зв'язків «порушення → санкція» [22]. У фінансах (звіти SEC) класифікація без навчання, за допомогою великих мовних моделей, визначає ризики та зобов'язання з точністю 85%. Підходить

для швидкого визначення типу судової справи [23]. У наукових статтях статистичний метод Yet Another Keyword Extractor (YAKE) – це швидкий, безнавчальний алгоритм для автоматичного виділення ключових слів і фраз з тексту, швидко знаходить головні теми з точністю 75–85%. Корисно для аналізу цитувань у рішеннях [24]. У соціальних мережах (Twitter/X) модель T5 це універсальна модель, яка перетворює будь-який текст, витягує події та учасників у реальному часі з точністю 80%. Вона також дозволяє виконувати моніторінг згадок судових справ у медіа [25]. У технічній документації, наприклад у описах патентів (офіційних документах про винаходи), аналіз зв'язків між словами з подальшим застосуванням класичної моделі CRF дозволяє виділяти назву винаходу та імена авторів з точністю 90%. Цей самий підхід можна адаптувати для пошуку норм права та їх застосування у судових рішеннях [26].

Ці підходи з інших сфер дозволяють порівнювати та переносити рішення, наприклад, з медичною сфери до юридичної сфери.

Існуючі інструменти з готовими моделями для україномовних ресурсів досягають 75–80% точності при витягуванні ключової інформації без додаткового навчання [27].

Сучасні інструменти акцентують увагу на виділенні головних тез, що узагальнюють документ, як у системах скорочення судових рішень [11]. Пошук на основі словників знань (онтології) структурує сутність документу [4]. У 2024 році запропоновано комбіновану модель BiLSTM-CRF з урахуванням нечіткості для пошуку метафор і складних термінів, що підвищує точність на 10–15% [9]. Для автоматичного виділення логіки рішень використовують BERT разом з BiLSTM-CRF, що дозволяє знаходити правила «якщо – то» для моделювання [30]. Ці методи доповнюють RAG, додаючи глибше розуміння змісту [10].

План проведеного дослідження включає відбір даних, їх підготовку, розмітку, навчання моделей та оцінку результатів. Експеримент відтворюваний на стандартному обладнанні з Python 3.10, бібліотеками Hugging Face Transformers, FAISS, scikit-learn та seqeval.

Набір даних сформовано з Єдиного державного реєстру судових рішень (ЄДРСР) за період 2023–2024 років. Загалом відібрано 500 унікальних судових рішень, що охоплюють цивільні (60%), кримінальні (25%) та адміністративні (15%) справи. Це забезпечує репрезентативність вибірки. Кожен документ – повний текст рішення у форматі TXT, очищений від метаданих (номер справи, дата публікації). Середня довжина – 500 слів, мінімальна – 150, максимальна – 2500. Загальний обсяг всіх документів сягає близько 250 тисяч слів.

Підготовка даних включала токенізацію (розбиття на слова та знаки), нормалізацію (приведення до нижнього регістру, видалення зайвих пробілів) та анонімізацію (заміна реальних імен на теги типу [ПОЗИВАЧ_1], [ВІДПОВІДАЧ_2] для захисту персональних даних). Кожне рішення

розмітовувалося на вісім типів сутностей, учасники (позивач, відповідач, суддя, свідок), норми права (стаття, частина, пункт), дати, місця, факти (події, суми), рішення (задоволено, відмовлено, частково), мотиви (аргументи), санкції (штраф, термін). Також позначено зв'язки між сутностями, наприклад «учасник → норма права» чи «норма права → санкція».

Набір поділено на три частини, 70% (350 документів) – для навчання моделей, 15% (75) – для перевірки під час налаштування, 15% (75) – для фінального тесту. Такий розподіл стандартний у машинному навчанні та запобігає перенавчанню.

Перевірено три різні методи витягування потрібної інформації. Перший – підхід на основі шаблонів, це простий пошук за заздалегідь підготовленими зразками (регулярними виразами) та словниками. Наприклад, шаблон для норм права — «ст.?\s*\d+» або «частина\s+\w+», словник організацій – «ТОВ», «ПАТ», «ФОП». Цей метод не потребує навчання, працює швидко, але жорсткий до варіацій у тексті. Другий метод являє собою модель на основі української версії BERT (UkBERT) з додатковим шаром для класифікації. Третій – метод доповнення контексту законом RAG, спочатку векторний пошук трьох найближчих статей законодавства з бази «Законодавство України» (FAISS, ембеддинги від Sentence-BERT), потім передача судового тексту + знайдених статей генеративній моделі (Llama-3-8B) з запитом, «Витягни ключову інформацію, учасники, норми, факти, рішення, мотиви, санкції».

Оцінка якості проводилася за трьома метриками, зрозумілими навіть без технічної підготовки. Точність – це відсоток правильних відповідей серед усіх, які система позначила як факти. Наприклад, якщо система знайшла 10 норм права, але 2 з них помилкові, точність – 80%. Повнота – відсоток знайдених фактів від усіх, що є в тексті насправді. Якщо в документі 15 учасників, а система знайшла 12 правильних, повнота – 80%. Загальна оцінка являє собою середнє гармонійне між точністю та повнотою, щоб уникнути переваги по кожному показнику. Розрахунок проводився окремо для сутностей (імена, дати, норми) та зв'язків між ними за допомогою бібліотек seqeval і scikit-learn. Кожен метод запускався тричі, а отримані результати усереднювалися.

Експеримент проведено на тестовій вибірці з 75 судових рішень, що становить 37500 слів. Середня довжина одного документа – 500 слів. Обробка виконувалася на сервері з графічним процесором NVIDIA A100. Кожен метод запускався тричі, результати усереднені. Час вимірювався від моменту завантаження тексту до отримання структурованої інформації.

Загальні результати такі, метод доповнення контексту законом RAG показав найкращі значення – 91% точності та 87% повноти для пошуку сутностей, що дає загальну оцінку 89%. Для зв'язків між сутностями – 86% точності, 82% повноти, загальна оцінка 84%. Час обробки – 0,35 секунди на документ.

Українська версія BERT досягла 88% точності та 84% повноти для сутностей, загальну оцінку 86%, для зв'язків – 83% і 79% загальна оцінка 81%, час – 0,25 секунди [28]. Підхід на основі шаблонів дав 75% точності та 69% повноти для сутностей загальна оцінка 72%, для зв'язків – 68% і 62% загальна оцінка 65%, але найшвидший – 0,05 секунди на документ.

За типами сутностей перевага RAG особливо помітна при пошуку норм права, 91% загальна оцінка проти 65% у шаблонів і 79% у BERT [29]. Це пояснюється тим, що модель бачить не лише посилання в рішенні, а й повний текст статті закону. Для учасників справи RAG досягає 94%, BERT – 90%, шаблони – 82%. Дати та місця, 90%, 87%, 78% відповідно. Рішення, 88%, 85%, 70%. Санкції, 87%, 82%, 68%.

Щодо довжини документа, RAG зберігає стабільність, для коротких текстів (менше 300 слів) – 90%, середніх (300–1000) – 88%, довгих (понад 1000) – 87%. BERT падає з 87% до 83%, шаблони – з 74% до 68%. Це показує, що зовнішній контекст допомагає навіть у складних випадках.

Приклади помилок ілюструють слабкі місця. Підхід на основі шаблонів не розпізнає «частина третя статті 190 Кримінального кодексу України», бо шукає лише «ст. 190 ч. 3». BERT плутає «стаття договору» і «стаття кодексу» у 12% випадків через схожість слів. RAG вирішує це, додаючи текст: «ст. 190 КК України – шахрайство».

Порівняння з ручним аналізом, юристи витрачають в середньому 22 хвилини на документ (за 10 експертами) [15]. Автоматизовані методи – від 0,05 до 0,35 секунди. Економія – від 3760 до 26 400 разів.

Проведене дослідження чітко доводить, що інтеграція зовнішнього нормативного контексту (RAG – це інструмент, який не вигадує, а шукає в твоїх документах і відповідає тільки за фактами) є найефективнішим способом автоматичного витягування ключової інформації з україномовних судових рішень. Цей підхід суттєво перевершує традиційні шаблони та моделі, які працюють лише з текстом документа, завдяки здатності «розуміти» зміст норм права, а не лише їхні посилання.

Головний висновок це якісне витягування інформації з юридичних текстів українською мовою неможливе без поєднання мовних моделей із базою законодавства. Самостійне використання готових моделей дає прийнятні результати, але додавання релевантних статей закону як контексту усуває більшість помилок інтерпретації, особливо при роботі з нормами права.

Важливим моментом є критична нестача анотованих даних для української юридичної мови. Існуючі набори орієнтовані на загальну мову, а спеціалізовані корпуси для судових рішень відсутні. Це гальмує розвиток моделей і пояснює, чому навіть найкращі підходи потребують додаткового навчання. Створення великого національного корпусу розмічених судових

рішень має стати стратегічним завданням для розвитку юридичного напрямку ШІ в Україні.

Нарешті, дослідження підкреслює необхідність співпраці між юристами, розробниками та державними органами. Юристи потрібні для розмітки законодавчих даних, розробники – для створення зручних інтерфейсів, держава – для забезпечення доступу до структурованих джерел законотворчої інформації.

Отже, проведена робота не просто демонструє ефективний метод, а відкриває шлях до системної цифровізації української юриспруденції, де штучний інтелект стане повсякденним помічником, забезпечуючи швидкість, точність і рівний доступ до правової інформації.

Список використаних джерел:

1. ЄДРСР. Статистика 2025. https://reyestr.court.gov.ua/.
2. Мін'юст України. Звіт про цифровізацію 2024. https://minjust.gov.ua/digital-report-2024.
3. EU e-Justice Portal. Digital Justice Systems. https://e-justice.europa.eu.
4. Bhattacharyya A. et al. (2023). Merger Agreement Dataset. EMNLP 2023. https://aclanthology.org/2023.emnlp-main.1019.pdf.
5. Kalamkar P. et al. (2022). Named Entity Recognition in Indian Court Judgments. NLLP 2022. https://aclanthology.org/2022.nllp-1.15.pdf
6. Martinez-Gil J. (2025). Legal Citation Detection in UK Judgments. EMNLP 2025. https://aclanthology.org/2025.emnlp-main.1361.pdf
7. Angelidis I. et al. (2023). Legal Citation Extraction. ACL 2023. https://aclanthology.org/2023.findings-acl.123
8. Glaser I. et al. (2024). Event Extraction in Legal Texts. NLLP 2024.
9. Chalkidis I. et al. (2022). LexGLUE: A Benchmark for Legal Language Understanding. ACL 2022. https://aclanthology.org/2022.acl-long.297.pdf
10. Zhong Y., Litman D. (2022). Structural Computation for Case Summarization. NLLP 2022. https://aclanthology.org/2022.nllp-1.30.pdf
11. Galgani F. et al. (2023). Catchphrase Extraction for Legal Document Summarization. NLLP 2023. https://aclanthology.org/2023.nllp-1.12.pdf
12. Sanchez J. et al. (2025). Monetary Sanction Extraction. EMNLP 2025.
13. Ivanenko O. (2025). Analysis of Ukrainian Court Decisions Structure. UNLP 2025.
14. Quinta de Castro P. V., Da Silva N. F. F. (2025). Labor Lex: Information Extraction from Brazilian Labor Law. NLLP 2025. https://aclanthology.org/2025.nllp-1.14.pdf
15. Panchenko E. et al. (2022). Claim and Regulation Extraction for COVID-19. LREC 2022. https://aclanthology.org/2022.lrec-1.50.pdf
16. Bhattacharyya A. et al. (2025). Information Extraction from Visually Rich Documents. ACL 2025. https://aclanthology.org/2025.acl-long.844.pdf
17. Jungiewicz M., Łopuszyński G. (2022). Keyword Extraction from Polish Legal Texts. Springer NLP.

18. Halama P. et al. (2022). Classification of Polish Court Judgments Using N-grams and Stemming. Archives of Acoustics.
19. IEEE Access. (2024). BiLSTM-CRF with Fuzzy Logic for Legal Metaphor Extraction.
20. Dragoni M. et al. (2023). Ontology-Based Extraction in Polish Legal Texts. Springer.
arXiv. (2025). Polish BERT for Legislative Analysis.
21. Wang Y. et al. (2024). Graph-Based Clinical Entity Extraction. ACL BioNLP.
22. Li H. et al. (2025). Zero-Shot Risk Classification in SEC Filings. NAACL Industry.
23. Campos R. et al. (2023). YAKE for Scientific Keyphrase Extraction. ECIR.
24. Zhang L. et al. (2024). Event Extraction from Social Media with T5. EMNLP.
25. Liu Z. et al. (2023). Dependency Parsing for Patent Claim Extraction. IP&M.
26. Codesignal. (2025). Legal Information Extraction with Text Processing Libraries. https://codesignal.com/learn/courses/practical-applications-of-text-processing-for-real-life-tasks/lessons/information-extraction-from-legal-documents
27. Osyvokon. (2025). Ukrainian Language Resources Catalog. https://github.com/osyvokon/ukrainian-language-resources
28. UNLP. (2025). Ukrainian Natural Language Processing Conference. https://unlp.org.ua/
29. IEEE Access. (2024). Decision Model Extraction Using BERT and BiLSTM-CRF.

ЄВРОПЕЙСЬКИЙ ЗАГАЛЬНИЙ РЕГЛАМЕНТ ЗАХИСТУ ДАНИХ (GDPR): НАПРЯМИ ДІЇ, ВПЛИВ І ВИКЛИКИ

Шевчук Марія

студентка 1 курсу факультету прокуратури та слідства (кримінальної юстиції) Національного університету «Одеська юридична академія»

У сучасному цифровому світі персональні дані стали однією з найцінніших форм цифрової інформації, що визначає не лише приватність людини, а й рівень її інформаційної безпеки та захищеності в умовах розвитку електронного суспільства. Стрімке поширення цифрових технологій, зростання ролі великих даних (Big Data) і активне використання штучного інтелекту зумовили потребу у посиленні правових механізмів регулювання процесів збору, обробки, зберігання та передачі персональної інформації. У відповідь на ці виклики Європейський Союз ухвалив Загальний регламент про захист даних — GDPR (Regulation (EU) 2016/679), який став основоположним актом цифрового права в Європі [1].

Регламент Європейського Союзу 2016/679, відомий як General Data Protection Regulation (GDPR), є ключовим правовим документом у сфері захисту персональних даних на території ЄС. Він набув чинності 25 травня 2018 року та став однією з найбільш масштабних реформ у галузі цифрового законодавства. Головною метою GDPR є встановлення уніфікованих стандартів обробки персональних даних фізичних осіб, підвищення прозорості

процесів обробки інформації та зміцнення відповідальності організацій, які здійснюють такі операції.

Загальний регламент про захист даних установлює єдині правила для всіх держав-членів ЄС, враховуючи сучасні технологічні зміни, що суттєво вплинули на методи збирання, зберігання та використання особистої інформації. Регламент покликаний узгодити правові норми із потребами цифрової епохи, яка визначається стрімким розвитком Інтернету, соціальних мереж, хмарних сервісів та автоматизованих інформаційних систем [2].

Однією з ключових особливостей GDPR є його екстериторіальна дія: норми Регламенту поширюються на всі організації, що обробляють персональні дані громадян ЄС, незалежно від країни реєстрації. Це стосується як комерційних, так і безкоштовних цифрових послуг, а також будь-якої діяльності з моніторингу поведінки користувачів у мережі. Правила Регламенту поширюються і на державні установи, які надають послуги в межах електронного урядування.

GDPR ґрунтується на принципі повної інформованості користувачів щодо того, як і з якою метою обробляються їхні персональні дані. Кожна особа має право отримати інформацію про контролера даних, характер обробки, а також можливість висловлювати заперечення проти таких операцій. Для організацій виконання вимог GDPR має також репутаційний вимір, оскільки відповідальне ставлення до приватності даних підвищує довіру користувачів та конкурентоспроможність компанії на ринку.

Важливим досягненням Регламенту є чітке визначення учасників процесу обробки даних. Згідно зі статтею 4 GDPR, контролер — це фізична або юридична особа чи орган влади, що визначає мету та способи обробки даних. Обробник даних — структура, яка здійснює операції з даними від імені контролера, наприклад провайдери хмарних технологій [3].

Суб'єктом даних є фізична особа, інформація про яку обробляється. До спеціальних категорій належать дані про расове походження, політичні переконання, релігію, членство у профспілках, стан здоров'я, біометричні та генетичні характеристики.

Регламент визначає розширене коло прав суб'єктів даних: право на доступ до інформації, виправлення даних, заборону обробки, перенесення даних та подання заперечення проти автоматизованих рішень. Особливе значення має «право на забуття», яке дозволяє вимагати видалення персональної інформації, що більше не відповідає меті обробки або порушує права людини.

Суттєвою інституційною новацією GDPR стало запровадження посади уповноваженого з питань захисту даних (Data Protection Officer, DPO). Обов'язок призначення DPO виникає у випадках, коли діяльність організації передбачає систематичний або масштабний моніторинг персональних даних.

Для державних інституцій наявність DPO є обов'язковою, тоді як приватні компанії визначають потребу залежно від рівня ризику обробки [4].

Контроль за дотриманням норм GDPR здійснюється національними органами із захисту даних (Data Protection Authorities, DPA). Ці органи мають повноваження проводити перевірки, накладати штрафи, вимагати усунення порушень або обмеження діяльності контролера чи обробника. Європейська рада із захисту даних (European Data Protection Board) координує роботу національних регуляторів і забезпечує єдину практику застосування норм Регламенту.

Особливу увагу привертають санкції, передбачені Регламентом. Залежно від характеру та серйозності порушення, штрафи можуть досягати до 20 мільйонів євро або 4% глобального обороту компанії. Менш серйозні порушення караються штрафами до 10 мільйонів євро або 2% обороту. Такі значні суми стимулюють компанії впроваджувати високі стандарти цифрової безпеки та відповідності.

У останні роки роль GDPR набуває глобального значення. Його екстериторіальні положення змушують міжнародні компанії адаптувати внутрішні процедури обробки даних навіть у країнах, що не підпадають під юрисдикцію ЄС. Це спричинило формування так званого «ефекту Брюсселя», коли національні законодавства різних держав поступово вирівнюються відповідно до європейських стандартів приватності.

Водночас практика застосування Регламенту демонструє низку викликів: повільні процедури розгляду справ національними регуляторами, нестачу прецедентного права, а також фінансові та технічні труднощі для малих і середніх підприємств. Це формує потребу у розробленні ефективних систем цифрової відповідності (digital compliance) та створенні адаптивних національних політик захисту даних.

Отже, GDPR є одним з найефективніших сучасних нормативно-правових актів у сфері контролю за обробкою персональних даних. Його положення забезпечують високий рівень захисту прав суб'єктів даних, встановлюють жорсткі вимоги до організацій і формують комплексну систему контролю на рівні ЄС. Для України адаптація національного законодавства до стандартів GDPR є важливим кроком до зміцнення кібербезпеки та інтеграції в європейський цифровий простір.

Список використаних джерел

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR) [Електронний ресурс]. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 06.11.2025).

2. General Data Protection Regulation (GDPR) — Summary // EUR-Lex [Електронний ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A310401_2 (дата звернення: 07.11.2025).
3. What is GDPR? // GDPR.EU — Official EU GDPR Information Portal [Електронний ресурс]. URL: https://gdpr.eu/what-is-gdpr (дата звернення: 10.11.2025).
4. European Data Protection Board (EDPB) — official documentation, guidelines and coordination mechanisms [Електронний ресурс]. URL: https://edpb.europa.eu (дата звернення: 11.11.2025).
5. Voigt P., Von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing, 2017. URL: https://link.springer.com/book/10.1007/978-3-319-57959-7 (дата звернення: 11.11.2025).

Ключові слова: захист персональних даних; GDPR; цифрове регулювання; екстериторіальна дія; цифрова відповідність; кібербезпека.
Keywords: personal data protection; GDPR; digital regulation; extraterritorial scope; digital compliance; cybersecurity.personal data protection; GDPR; digital regulation; extraterritorial scope; digital compliance; cybersecurity.

Науковий керівник: к.ю.н. доцент Чанишев Р.І.

ЛІЦЕНЗУВАННЯ ТА УПРАВЛІННЯ ПРАВАМИ НА ЦИФРОВИЙ МУЛЬТИМЕДІЙНИЙ КОНТЕНТ: ІНТЕГРАЦІЯ ТЕХНІЧНИХ ЗАСОБІВ КОНТРОЛЮ У ПРАВОВІ ПРОЦЕДУРИ

Овчинников Микола
асистент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Цифровізація обігу мультимедійного контенту призвела до того, що правові механізми ліцензування та захисту авторських прав дедалі частіше реалізуються через інформаційні системи, а питання кібербезпеки й захисту інформації стають невід'ємною частиною правової процедури. У межах дисертаційного напряму з розробки інформаційної системи захисту інтелектуальної власності на мультимедійні дані пропонується розглядати ліцензію як сукупність машиночитних правил використання, доповнених технічними контролями цілісності та доказовості.

Передумовою інтеграції технічного контролю в правові процедури є стандартизація опису прав. MPEG-21 Rights Expression Language (REL) демонструє можливість формалізованого опису прав, обмежень та умов використання у форматі, придатному для автоматизованого виконання у DRM-системах і сервісах розповсюдження контенту [1].

З позицій моделювання захисту прав у кіберпросторі корисним є багаторівневий погляд на DRM. Чотиришарова модель безпеки DRM (довіра,

управління правами, примус виконання прав, захист контенту) дозволяє узгодити юридичні рішення (хто і що може робити) та технічні засоби (як саме це забезпечується), що важливо для побудови контролів безпеки та аудитності системи [2].

Технічний шар доказовості у системі може включати: (а) фінгерпринт/хеш для фіксації стану об'єкта; (б) робастний водяний знак, який пов'язує об'єкт із ідентифікатором правовласника/ліцензії; (в) незмінний журнал подій для відстеження доступу, передачі та модифікацій. Метадані-орієнтовані схеми водяного маркування показують практичну придатність прив'язки даних про авторство/права до контенту з урахуванням типових перетворень (стискання, ресайз) [3].

Окремий тренд – поєднання smart legal contracts (юридично значущих умов) зі смарт-контрактами для нотаризації подій, трансферу прав та автоматизації роялті. Така модель підсилює доказовість за рахунок незмінності реєстру та дозволяє технічно пов'язати договір, версію контенту і факт передачі/використання [4].

Разом із тим, блокчейн-підхід потребує уваги до конфіденційності й мінімізації даних: у публічному шарі доцільно залишати лише хеші/таймстемпи/ідентифікатори, тоді як деталі ліцензії та персональні дані – зберігати в захищеному сховищі з контрольованим доступом. Практичні огляди застосування блокчейна і смарт-контрактів для авторського права підкреслюють значення сумісності з платформами та чітких політик доступу [5].

Огляд сучасних досліджень DRM також вказує, що автоматизація виявлення порушень (зокрема AI/ML-інструментами) підвищує ефективність, але висуває вимоги до прозорості політик, пояснюваності рішень та коректної фіксації доказів. Для нормативно-правового напряму це означає необхідність формалізувати «ланцюг доказів» у межах системи та визначити ролі/повноваження учасників [6].

Додатково до зазначеного, практична реалізація «ланцюга доказів» потребує узгодження технічних артефактів із процесуальними вимогами: які саме дані зберігаються, як забезпечується їх цілісність, хто має доступ і в який спосіб підтверджується автентичність джерела. Доцільно передбачити стандартизований пакет доказів (хеш/фінгерпринт, ідентифікатор водяного знака, часові мітки, журнали подій, версії алгоритмів і параметри перевірки), а також регламент його формування та передачі для зовнішніх сторін (платформи, правовласник, експерт). Така стандартизація зменшує ризик неоднозначної інтерпретації результатів і забезпечує відтворюваність перевірок у межах правового спору.

На рис. 1 узагальнено інтеграцію технічних засобів контролю в ланцюг правової процедури ліцензування: від первинної реєстрації та формування

фінгерпринта/водяного знака – до укладення договору, нотаризації подій і підготовки доказової бази у разі спору.

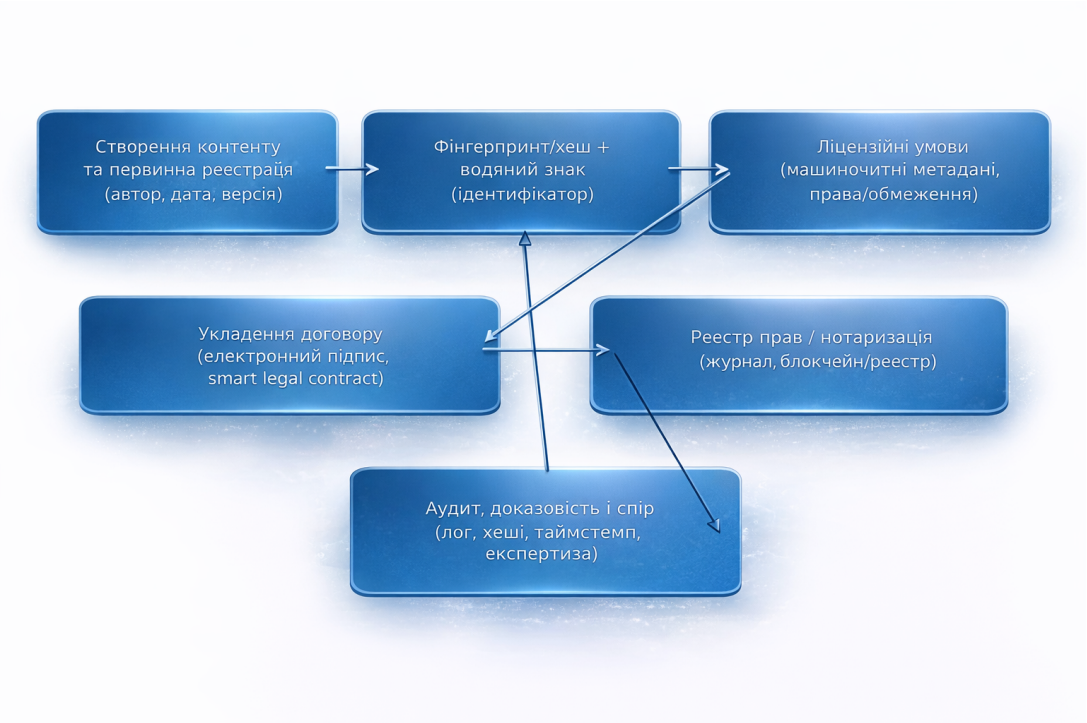

Рис. 1. Інтеграція технічних засобів контролю у правову процедуру ліцензування.

Нижче наведено узагальнену матрицю ролей/каналів і метрик, яку можна використати як основу «playbook» реагування (табл. 1).

Табл. 1. Відповідність правової процедури та технічних контролів у системі.

Етап/процедура	Технічний інструмент	Яке правове питання підсилює	Ризики та мінімізація
Ідентифікація	Хеш/фінгерпринт	Належність версії	Колізії -> дублювання контролів
Прив'язка прав	Водяний знак + ID	Походження/авторство	Втрати сигналу -> робастність
Умови ліцензії	MPEG-21 REL/метадані	Однозначність прав	Помилки -> валідація/версії
Договір/передача	Е-підпис/контракт	Дійсність волі	Компрометація -> MFA, ротація
Нотаризація	Блокчейн хеш+час	Факт події/пріоритет	Конфіденційність -> мінімізація
Аудит/спір	WORM-журнал	Ланцюг доказів	Цілісність -> підпис/резервування

Інтеграція технічних засобів контролю у процедури ліцензування перетворює ліцензію на керований життєвий цикл цифрового активу: реєстрація та ідентифікація (хеш/фінгерпринт, водяний знак) → договір → нотаризація подій → аудит. Це підвищує юридичну визначеність і скорочує час реагування на порушення. Для інформаційної системи критичні: машиночитні й версіоновані умови ліцензії, доказова цілісність журналів подій і прив'язка операцій до конкретної версії контенту, мінімізація даних і розмежування доступу (публічні хеші/таймстемпи та приватні деталі ліцензії). Технічні контролі підсилюють правові механізми, забезпечуючи їх виконуваність і відтворюваність у кіберпросторі.

Список використаної літератури:

1. Wang X. MPEG-21 Rights Expression Language: enabling interoperable DRM. IEEE MultiMedia. 2004. DOI: 10.1109/MMUL.2004.31.
2. Diehl E. A four-layer model for security of DRM (DRM '08). 2008. DOI: 10.1145/1456520.1456527.
3. Huang H., Fang W. Metadata-based image watermarking for copyright protection. Simulation Modelling Practice and Theory. 2010. DOI: 10.1016/j.simpat.2009.09.004.
4. Ferro E., Saltarella M., Rotondi D., et al. Digital assets rights management through smart legal contracts. Blockchain: Research and Applications. 2023. DOI: 10.1016/j.bcra.2023.100142.
5. Frattolillo A., Petitt J., Kalsi A., et al. Blockchain and smart contract for copyright management. Future Internet. 2024. DOI: 10.3390/fi16050169.
6. Feng X., Pan Y., Xiao N. Digital rights management: a review. Neurocomputing. 2025. DOI: 10.1016/j.neucom.2025.131672.

Ключові слова: ліцензування, цифрові права, DRM, цифровий водяний знак, смарт-контракти, доказовість, журнал подій, кібербезпека, захист інформації.
Keywords: licensing, digital rights, DRM, digital watermarking, smart contracts, evidentiary integrity, audit log, cybersecurity, information protection.

Науковий керівник: к.т.н., доцент Ахмаметьєва Г.В.

СТРАТЕГІЧНІ ТА ТЕХНІЧНІ ЗАСАДИ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

Костіна Олександра

студентка 1 курсу факультету прокуратури та слідства (кримінальної юстиції) Національного університету «Одеська юридична академія»

Кібербезпека набуває виняткового значення для будь-якої організації, незалежно від її сфери діяльності. Зі збільшенням кількості користувачів, розширенням мережевої інфраструктури, підключенням нових пристроїв та програмних рішень, а також зростанням обсягів інформації, що обробляються,

питання захисту даних стає одним із провідних аспектів забезпечення стабільної та безпечної роботи [1].

Особливо актуальним є захист конфіденційної інформації: персональних даних працівників, клієнтів, фінансової документації, комерційних таємниць і стратегічних рішень.

Сучасні кіберзагрози стають дедалі витонченішими. Зловмисники застосовують фішинг, соціальну інженерію, шкідливе програмне забезпечення та програми-вимагачі, атакують мережеву інфраструктуру й бази даних [2].

У результаті будь-яка організація, незалежно від розміру чи напрямку діяльності, може стати об'єктом кібератаки, що призводить до значних фінансових втрат, репутаційних ризиків або навіть до зупинки діяльності.

Тому питання кібербезпеки виходить за межі технічного виміру — воно стає стратегічним напрямом управління організацією. Важливо не лише впроваджувати сучасні технічні засоби захисту, а й формувати культуру інформаційної безпеки серед працівників, забезпечувати постійне навчання персоналу, моніторинг потенційних загроз і оперативне реагування на інциденти. Лише комплексний підхід до побудови системи кіберзахисту дозволить ефективно протистояти новим викликам цифрової ери та гарантувати стабільність функціонування організації в умовах зростаючих кіберризиків.

У законодавчому полі України, зокрема в Законі України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як комплексна система захисту життєво важливих інтересів людини, суспільства та держави під час використання кіберпростору [3].

Це поняття охоплює не лише технічну безпеку інформаційних систем, а й забезпечення сталого розвитку інформаційного суспільства, створення безпечного цифрового середовища. Кібербезпека передбачає своєчасне виявлення, попередження і нейтралізацію як реальних, так і потенційних загроз, які можуть завдати шкоди національним інтересам України.

Основна мета забезпечення кібербезпеки — збереження цілісності, конфіденційності та доступності інформації, запобігання кібератакам, кіберзлочинам, несанкціонованому втручанню в роботу державних і приватних інформаційних систем. У межах державної політики кібербезпека стає складовою національної безпеки, оскільки розвиток цифрових технологій породжує нові ризики та виклики. Забезпечення належного рівня кіберзахисту сприяє підвищенню довіри громадян до державних інституцій, розвитку електронного урядування, зміцненню обороноздатності країни та захисту інформаційного суверенітету.

Алгоритмічні та технічні аспекти кібербезпеки охоплюють розробку, впровадження і вдосконалення технологічних засобів захисту інформації у цифровому середовищі. Зростаючі обсяги даних і кількість мережевих

взаємодій вимагають вдосконалених алгоритмічних підходів та технічних рішень, що формують основу ефективної системи кіберзахисту.

Алгоритмічні аспекти включають використання математичних методів, логічних структур і обчислювальних процесів для забезпечення цілісності, конфіденційності й доступності інформації. Це алгоритми шифрування (симетричного й асиметричного типу), цифровий підпис, хешування, автентифікація користувачів, а також методи виявлення вторгнень та аномалій у мережевому трафіку. Наприклад, алгоритми RSA, AES, SHA-256 або новітні квантово-стійкі методи криптографії є ключовими у захисті обміну інформацією. Завдяки розвитку штучного інтелекту й машинного навчання алгоритмічний компонент кібербезпеки постійно вдосконалюється, що дає змогу прогнозувати та запобігати загрозам ще до їх реалізації.

Технічні аспекти стосуються практичної реалізації алгоритмів і інструментів захисту в комп'ютерних системах і мережах. Сюди належать апаратне й програмне забезпечення, системи виявлення вторгнень (IDS/IPS), брандмауери, антивірусні програми, засоби шифрування трафіку, системи контролю доступу, резервного копіювання та відновлення даних. Також важливі технології багатофакторної автентифікації, VPN, хмарні системи захисту та централізовані системи управління безпекою (SIEM).

Взаємозв'язок алгоритмічних і технічних аспектів визначає ефективність кіберзахисту: навіть найпотужніший алгоритм шифрування не забезпечить належного рівня безпеки без правильної технічної реалізації та налаштування системи. Тому ключовим завданням фахівців є інтеграція теоретичних моделей захисту з практичними рішеннями, здатними оперативно реагувати на загрози.

У найближчі роки важливою тенденцією стане інтеграція кібербезпеки з технологіями штучного інтелекту, автоматизації захисту та аналітики кіберзагроз на базі великих даних. Організації, які впроваджуватимуть автоматизовані системи реагування на інциденти, симуляції атак і проактивний захист — отримають стратегічну перевагу [4].

Крім того, соціальний аспект кібербезпеки набуває зростаючого значення: формування цифрової культури безпеки серед працівників, регулярне навчання й підвищення кіберграмотності стають критичними елементами будь-якої програми захисту. Людський фактор залишається одним із найслабших місць у системі — у багатьох випадках 68 % інцидентів пов'язані з людською помилкою.

Список використаних джерел

1. 40+ Data Breach Statistics 2025: Trends & Key Threats [Електронний ресурс]. URL: https://deepstrike.io/blog/data-breach-statistics-2025 (дата звернення: 09.11.2025).

2. Top Cybersecurity Statistics for 2025 [Електронний ресурс]. URL: https://www.cobalt.io/blog/top-cybersecurity-statistics-2025 (дата звернення: 09.11.2025).
3. Cyber Security Breaches Survey 2025 [Електронний ресурс]. URL: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025 (дата звернення: 09.11.2025).
4. Global Cybersecurity Outlook 2025 [Електронний ресурс]. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (дата звернення: 09.11.2025).

Ключові слова: кібербезпека; цифрова трансформація; захист даних; технічні засоби захисту; алгоритмічні методи; людський фактор; бізнес-управління безпекою.
Keywords: cybersecurity; digital transformation; data protection; technical security measures; algorithmic methods; human factor; security management.

Науковий керівник: к.ю.н. доцент Чанишев Р.І.

ШТУЧНИЙ ІНТЕЛЕКТ І ФІНАНСОВА СТАБІЛЬНІСТЬ: КЛЮЧОВІ ВИСНОВКИ КОМІТЕТУ З ФІНАНСОВОЇ ПОЛІТИКИ ВЕЛИКОЇ БРИТАНІЇ

Мовчан Анастасія
студентка 1 курсу факультету цивільної та господарської юстиції Національного університету «Одеська юридична академія»

Штучний інтелект (ШІ) стає одним із головних факторів, що змінюють фінансовий сектор. Він впливає на те, як працюють банки, страховики та інші фінансові установи, а також на те, які ризики виникають у всій фінансовій системі. У квітні 2025 року Комітет з фінансової політики Банку Англії опублікував спеціальну доповідь серії Financial Stability in Focus, у якій проаналізував, як саме ШІ може впливати на фінанси Великої Британії [1].

У документі зазначено, що ШІ — це не лише інструмент для підвищення ефективності. Він також може створювати нові ризики, тому за його впровадженням потрібно уважно стежити та вчасно реагувати на можливі загрози. Комітет підкреслює, що ШІ має властивості «технології широкого застосування», тобто може використовуватися майже скрізь — від обслуговування клієнтів до аналізу складних фінансових даних. Це здатне суттєво підвищити продуктивність завдяки автоматизації рутинних завдань, швидшому аналізу інформації та створенню персоналізованих фінансових сервісів.

Щоб оцінити реальний стан впровадження ШІ, Комітет проаналізував результати спільного опитування Банку Англії та Управління з фінансової поведінки, проведеного у 2024 році. Опитування показало, що 75 % фінансових установ уже використовують ШІ, а ще 10% планують

впровадження протягом трьох років. Найпоширеніші сфери застосування — оптимізація внутрішніх процесів, боротьба з фінансовим шахрайством і кіберзахист [2].

У доповіді ШІ розглядають з точки зору впливу на стійкість усієї фінансової системи. Простими словами, Комітет оцінює, чи допоможе ШІ фінансовому сектору краще витримувати економічні потрясіння, чи навпаки — зробить його вразливішим. Для цього визначено чотири основні напрями: використання ШІ у фінансових рішеннях банків і страховиків, його вплив на фінансові ринки, залежність від зовнішніх технологічних компаній та зміни у сфері кібербезпеки [3].

Перший напрям стосується того, як ШІ застосовують у таких ключових процесах, як кредитування, оцінка ризиків, визначення вартості фінансових продуктів. ШІ дозволяє банкам працювати з великими обсягами даних, точніше оцінювати позичальників і робити послуги доступнішими. Однак це створює і нові ризики. Наприклад, складні моделі можуть давати результати, які важко пояснити. Якщо багато установ використовують схожі моделі, помилка в одній з них може повторитися всюди, що здатне викликати широкі проблеми — так звані «системні дисбаланси», тобто збій у рівновазі всієї фінансової системи [4].

Другий напрям — вплив ШІ на фінансові ринки. Зокрема, це стосується алгоритмічної торгівлі, де рішення приймають комп’ютерні програми. Такі системи можуть робити ринок ефективнішим, швидше реагувати на інформацію. Але є й ризики. Якщо багато алгоритмів реагують однаково, це може призвести до «проциклічної поведінки» — коли учасники ринку масово діють в один бік. У періоди нестабільності це здатне збільшити «волатильність», тобто різкі коливання цін, що ускладнює торгівлю та може створити проблеми з ліквідністю. Також ШІ може виявляти нестандартні можливості для заробітку, які інколи можуть бути схожими на маніпуляції, тому регуляторам доведеться змінювати підхід до нагляду [5].

Третій напрям пов'язаний із тим, що багато фінансових установ використовують сторонні ШІ-сервіси, хмарні платформи та моделі. За опитуванням 2024 року, третина випадків використання ШІ залежить від таких постачальників. Проблема в тому, що кілька великих компаній контролюють більшу частину ринку. Це означає: якщо одна з них зіткнеться зі збоєм, значна частина фінансових установ може одночасно втратити доступ до важливих систем. Таку ситуацію вважають «системним операційним ризиком». Саме тому у Великій Британії вже розглядають ідею спеціального регулювання найбільших постачальників технологій.

Четвертий напрям — кібербезпека. Тут ефект двоякий. З одного боку, ШІ допомагає фінансовим установам краще виявляти загрози, швидше реагувати на них і виявляти шахрайство. З іншого боку, зловмисники також

використовують ШІ: автоматизують атаки, створюють реалістичні фішингові повідомлення, складні підробки аудіо й відео, шукають вразливості у системах [6]. Крім того, ШІ-системи самих фінансових компаній можуть стати слабким місцем, якщо не інтегровані у загальну систему кіберзахисту.

У доповіді також окреслено, як саме регулятори планують стежити за впровадженням ШІ. Вони використовуватимуть опитування, роботу спеціальних аналітичних груп, результати перевірок та інші джерела даних. У Великій Британії вже розробляють додаткові нормативні документи, що мають допомогти краще керувати ризиками ШІ. А на міжнародному рівні враховуються рекомендації Ради з фінансової стабільності, яка ще у 2017 році попереджала про можливі наслідки використання ШІ у фінансах.

Також у доповіді зазначено, що фінансова політика має бути гнучкою. Якщо роль ШІ і надалі зростатиме, можуть знадобитися нові інструменти: наприклад, додаткові перевірки моделей на стійкість до стресових ситуацій, контроль за залежністю від великих технологічних компаній, підсилення вимог до операційної стійкості та кіберзахисту.

Загалом FPC підкреслює, що ШІ приносить фінансовому сектору значні переваги: підвищення продуктивності, створення нових послуг, кращі можливості боротьби з шахрайством. Але одночасно наголошує, що ШІ може створити нові загрози, і тому потрібен продуманий підхід до регулювання. Це дозволить розвивати сучасні технології без ризику для стабільності всієї фінансової системи.

Список використаних джерел

1. Bank of England. Financial Stability in Focus: Artificial intelligence in the financial system. 09.04.2025. URL: https://www.bankofengland.co.uk/financial-stability-in-focus/2025/april-2025 (дата звернення: 06.11.2025).
2. Bank of England; Financial Conduct Authority. Artificial intelligence in UK financial services – 2024. 21.11.2024. URL: https://www.bankofengland.co.uk/report/2024/artificial-intelligence-in-uk-financial-services-2024 (дата звернення: 06.11.2025).
3. UK Financial Stability in Focus report: AI in the financial system. A&O Shearman FinReg Blog, 09.04.2025. URL: https://finreg.aoshearman.com/UK-Financial-Stability-in-Focus-report-AI-in-the-?utm_source (дата звернення: 06.11.2025).
4. Bank of England; Prudential Regulation Authority; Financial Conduct Authority. DP5/22 – Artificial Intelligence and Machine Learning. Discussion Paper 5/22, 11.10.2022. URL: https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence (дата звернення: 06.11.2025).
5. Financial Stability Board. Artificial intelligence and machine learning in financial services: Market developments and financial stability implications. 01.11.2017. URL: https://www.fsb.org/uploads/P011117.pdf (дата звернення: 06.11.2025).
6. Treacy S., Qemali E. Bank of England considers financial stability implications of AI. Linklaters Financial Regulation Blog, 29.04.2025. URL: https://financialregulation.linklaters.com/post/102k9ri/bank-of-england-considers-financial-stability-implications-of-ai (дата звернення: 06.11.2025).

Ключові слова: штучний інтелект; фінансова стабільність; Комітет з фінансової політики; системні ризики; регулювання фінансового сектору.
Keywords: artificial intelligence; financial stability; Financial Policy Committee; systemic risks; financial sector regulation.

Науковий керівник: к.ю.н. доцент Чанишев Р.І.

AEVA 2018: РЕГУЛЯТОРНІ ЗАСАДИ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В ТРАНСПОРТНУ ІНФРАСТРУКТУРУ ВЕЛИКОЇ БРИТАНІЇ

Лозовій Вероніка
студентка 1 курсу факультету судового та міжнародного права
Національного університету «Одеська юридична академія»

Automated and Electric Vehicles Act 2018 (AEVA) є ключовим нормативним актом Великої Британії, який створює правову рамку для функціонування автоматизованих транспортних засобів та розвитку інфраструктури електричного транспорту. Закон визначає механізми відповідальності, стандарти безпеки, вимоги до оновлення програмного забезпечення та принципи інтеграції електричних і автоматизованих транспортних засобів у національну транспортну систему, що робить AEVA одним із перших нормативних документів, який враховує зв'язок правового регулювання та сучасних інформаційних технологій [1].

Центральною частиною AEVA є врегулювання питань, пов'язаних із використанням автоматизованих транспортних засобів. Автономні автомобілі використовують комплекс цифрових технологій, включно з алгоритмами штучного інтелекту, сенсорними системами та телеметричними даними. Саме тому AEVA закладає правові механізми визначення відповідальності у разі ДТП або технічного збою систем самокерування [2].

Важливо, що закон вводить офіційний перелік автоматизованих транспортних засобів, які допускаються до руху у режимі самокерування. Це означає, що алгоритмічні системи штучного інтелекту проходять окрему верифікацію щодо відповідності вимогам безпеки.

Одним із найбільш прогресивних положень AEVA є спеціальна модель страхової відповідальності для автоматизованих транспортних засобів. Закон встановлює, що якщо автомобіль працював у режимі самокерування, то у разі дорожньо-транспортної пригоди відповідальність за відшкодування шкоди покладається не на водія, а на страхову компанію. Це означає, що потерпілі отримують компенсацію швидше і без необхідності доводити провину конкретної особи. Після виплати страховик отримує право регресу — тобто може звернутися з вимогою відшкодувати понесені витрати до виробника

автомобіля або розробника програмного забезпечення, якщо причина аварії пов'язана з помилкою алгоритмів, несправністю сенсорів, некоректною інтеграцією оновлень або іншими технічними дефектами системи самокерування. Такий підхід змінює традиційну модель дорожньої відповідальності, оскільки юридична увага переноситься з поведінки людини-водія на технічний стан цифрової системи та алгоритмічну надійність транспортного засобу. Він також стимулює виробників приділяти більше уваги якості програмного забезпечення, тестуванню автономних функцій і забезпеченню кіберстійкості, адже саме ці чинники прямо впливають на потенційні юридичні ризики та фінансові наслідки для компаній.

AEVA також регулює оновлення програмного забезпечення, що є критично важливим для безпеки автоматизованих транспортних засобів. Закон передбачає обов'язок користувача встановлювати оновлення, а невиконання цього може стати підставою для відмови у страхових виплатах [3].

Другий великий блок AEVA стосується розвитку інфраструктури електричного транспорту, що є необхідною умовою для масштабного впровадження електромобілів. Закон деталізує вимоги до створення розгалуженої мережі зарядних станцій, зокрема обов'язковість встановлення пунктів заряджання на автозаправних комплексах, уздовж основних автомагістралей та у ключових транспортних вузлах.

AEVA також передбачає стандартизацію платіжних інтерфейсів: користувачі повинні мати можливість заряджати автомобіль без укладання довгострокових контрактів із конкретними операторами, використовуючи універсальні способи оплати. Це спрямовано на усунення бар'єрів для водіїв та створення рівних умов доступу до інфраструктури.

Окрему увагу приділено впровадженню «розумних» (smart) зарядних пристроїв, які здатні автоматично регулювати інтенсивність заряджання залежно від стану електромережі, тарифів, часу доби або рівня навантаження.

Такі пристрої інтегруються у цифрові енергетичні системи та можуть працювати у режимах оптимізації споживання — наприклад, заряджати автомобіль у години найнижчого навантаження або реагувати на сигнали системи управління енергорозподілом. Це дозволяє зменшити пікове навантаження на мережу, підвищити ефективність використання енергії та створити передумови для розвитку концепції «розумних» електромереж, тісно пов'язаних з інформаційними технологіями та цифровими платформами управління. [4].

У контексті штучного інтелекту AEVA стимулює розвиток інтелектуальних транспортних систем, які працюють на основі машинного навчання, аналізу великих даних та високоточних навігаційних алгоритмів.

Закон формує юридичні умови для взаємодії між державою, виробниками, страховими компаніями та IT-індустрією.

AEVA також закладає принципи кібербезпеки транспортних систем, оскільки автономні авто стають потенційними об'єктами кібератак. Закон визначає обов'язковість захисту даних, стійкості до втручань та оновлення безпекових модулів у програмному забезпеченні.

Крім того, AEVA має стратегічне значення для розвитку концепції «розумних міст». Автономні та електричні транспортні засоби вимагають інтеграції у цифрову дорожню інфраструктуру, що включає системи моніторингу, аналізу та прогнозування дорожніх ситуацій.

Отже, Automated and Electric Vehicles Act 2018 є стратегічно важливим нормативним актом, що формує правову основу для розвитку транспортних технологій нового покоління. Закон поєднує регулювання автономного транспорту, інфраструктури заряджання електротранспорту, цифрової безпеки та інтелектуальної інфраструктури, створюючи передумови для безпечної й ефективної інтеграції систем штучного інтелекту в транспортну сферу та забезпечуючи стабільність, надійність і безпеку функціонування транспортних систем у цифрову еру.

Список використаних джерел

1. Automated and Electric Vehicles Act 2018.. URL: https://www.legislation.gov.uk/ukpga/2018/18 (дата звернення: 06.11.2025).
2. The Automated and Electric Vehicles Act 2018: Briefing Paper CBP-8118. URL: https://researchbriefings.files.parliament.uk/documents/CBP-8118/CBP-8118.pdf (дата звернення: 06.11.2025).
3. Autonomous vehicles: legal and regulatory framework – United Kingdom. 2024. URL: https://uk.practicallaw.thomsonreuters.com/w-013-2663 (дата звернення: 06.11.2025).
4. Automated and Electric Vehicles Act 2018 Regulatory Report: July 2023 – December 2024. 10 березня 2025. URL: https://www.gov.uk/government/publications/automated-and-electric-vehicles-act-2018-regulatory-report-2024 (дата звернення: 06.11.2025).

Ключові слова: автономні транспортні засоби, електричний транспорт, штучний інтелект, інформаційні технології, правове регулювання.
Keywords: autonomous vehicles, electric transport, artificial intelligence, information technologies, legal regulation.

Науковий керівник: к.ю.н. доцент Чанишев Р.І.

ПРАВОВІ ІНСТРУМЕНТИ ЄС У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ РИНКУ МОБІЛЬНИХ ДОДАТКІВ

Волонтирець Анастасія

студентка 1 курсу факультету прокуратури та слідства (кримінальної юстиції) Національного університету «Одеська юридична академія»

Швидке розширення цифрової економіки та стрімке зростання кількості мобільних користувачів у світі призвели до істотного збільшення випадків появи шахрайських мобільних додатків, що маскуються під легітимні продукти в App Store та Google Play. Такі програми використовуються для викрадення персональних даних, несанкціонованих списань коштів, фішингу або прихованого нав'язування платних послуг. З огляду на ці загрози Європейський Союз формує комплексну політику цифрового регулювання, спрямовану на підвищення прозорості та відповідальності цифрових платформ, зокрема в межах Digital Services Act (DSA) та Digital Markets Act (DMA) [1].

ЄС створює уніфіковану нормативну базу, яка покладає на великі онлайн-платформи, включно з магазинами мобільних додатків, чітко визначені обов'язки щодо оцінювання та мінімізації ризиків поширення незаконного або шкідливого контенту. DSA встановлює вимогу впроваджувати системи виявлення та протидії потенційно небезпечним додаткам ще на етапі попередньої перевірки, що вимагає від App Store і Google Play розроблення ефективніших алгоритмів модерації [2].

Важливим напрямом є підвищення прозорості діяльності платформ. Згідно з нормами DSA, оператори магазинів мобільних додатків повинні регулярно публікувати звіти щодо видалення або блокування програм, а також надавати доступ до базових технічних даних для незалежних дослідників і наглядових установ [3]. Це дозволяє оцінювати реальні результати боротьби з шахрайськими продуктами та створює підзвітність для технологічних компаній.

Протягом 2024–2025 років Європейська комісія активно застосовує наглядові механізми, надсилаючи запити Apple та Google з вимогою надати інформацію про політики модерації, статистику скарг і процедури реагування на порушення [4]. Такий підхід переходить від декларування відповідальності платформ до реального контролю за виконанням вимог законодавства.

DMA запроваджує додаткові правила для так званих «гейткіперів» — великих технологічних компаній, які контролюють критично важливі цифрові екосистеми. Для Apple та Google це означає обмеження можливості зловживання ринковою владою, забезпечення рівного доступу сторонніх розробників і формування прозорих умов перевірки додатків. DMA передбачає відкритість екосистем, можливість встановлення додатків із зовнішніх

джерел, а також зобов'язує компанії гарантувати захист прав користувачів у випадках виявлення шахрайства [2].

Окремим пріоритетом ЄС є створення превентивних механізмів, спрямованих на зменшення ризику поширення шкідливих додатків. До них належать удосконалені системи верифікації розробників, перевірки автентичності програм, аналіз платіжних інтеграцій і посилений контроль за використанням API та персональних даних. У межах DSA також передбачено механізм «trusted flaggers» — авторизованих організацій, які мають право оперативно повідомляти платформи про небезпечні програми, забезпечуючи швидший процес реагування.

Додаткові вимоги ЄС також стосуються прозорості алгоритмів, що застосовуються платформами для ранжування, модерації й рекомендацій додатків. Оскільки значна частина завантажень у магазинах мобільних застосунків формуються через рекомендаційні системи, Європейський Союз наголошує на важливості відкритості їх базових принципів. DSA передбачає обов'язок пояснювати користувачам логіку роботи таких алгоритмів та надавати можливість відмови від персоналізованого ранжування. Це спрямовано на запобігання маніпуляціям, завдяки яким шахрайські програми можуть підвищувати видимість за рахунок викривлення метаданих чи рекламних механізмів.

Крім того, вагомим елементом європейської стратегії є підвищення відповідальності розробників додатків. Нормативні вимоги ЄС передбачають не лише контроль за платформами, а й зобов'язання незалежних розробників підтверджувати свою ідентичність, дотримуватися стандартів безпеки та оперативно реагувати на повідомлення про зловживання. Такий комплексний підхід, що поєднує регулювання платформ та відповідальність розробників, формує більш стійку модель захисту цифрового ринку та сприяє зниженню кількості шкідливих додатків у європейському цифровому середовищі.

Законодавство встановлює і вагомі санкції. У разі серйозних або систематичних порушень DSA передбачає штрафи до 6 % від глобального річного обороту компанії [5]. Це створює реальний фінансовий стимул для дотримання вимог та підтримки безпечного цифрового середовища.

Проблематика шахрайських додатків має не лише юридичну, а й технічну складову. Сучасні шахраї застосовують штучний інтелект для обходу традиційних систем виявлення, що ускладнює модерацію та потребує постійного вдосконалення алгоритмічних інструментів. Тому ЄС підкреслює важливість координації між платформами, фінансовими установами, телекомунікаційними компаніями та правоохоронними органами з метою створення єдиної системи кіберзахисту.

Перспективи розвитку європейського регулювання передбачають поєднання наглядових заходів із формуванням культури етичного

саморегулювання платформ. ЄС прагне підтримувати баланс між безпекою користувачів і свободою підприємницької діяльності, одночасно забезпечуючи конкурентність цифрового ринку та високий рівень довіри до мобільних екосистем.

Отже, протидія шахрайським додаткам у магазинах App Store і Google Play є важливою складовою ширшої стратегії цифрової безпеки ЄС. Інтеграція вимог Digital Services Act і Digital Markets Act формує системний підхід до регулювання платформ, створює чіткі правила відповідальності, забезпечує прозорість і сприяє зміцненню Єдиного цифрового ринку.

Список використаних джерел

1. Digital Services Act: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Official Journal of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065 (дата звернення: 13.11.2025).
2. Digital Markets Act: Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector. Official Journal of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925 (дата звернення: 13.11.2025).
3. European Commission. The Digital Services Act and Digital Markets Act: New Rules for Online Platforms. Brussels, 2023. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (дата звернення: 13.11.2025).
4. European Commission. Questions to Apple and Google on Fraudulent Apps. Press release, 2025. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_541 (дата звернення: 13.11.2025).
5. European Parliament. Fact Sheet: Enforcement and Penalties under the DSA. Brussels, 2023. URL: https://www.europarl.europa.eu/factsheets/en/sheet/214/digital-services-act (дата звернення: 13.11.2025).

Ключові слова: цифрове регулювання; Digital Services Act; Digital Markets Act; шахрайські додатки; мобільні платформи; кібербезпека; модерація контенту; європейське законодавство.

Keywords: digital regulation; Digital Services Act; Digital Markets Act; fraudulent apps; mobile platforms; cybersecurity; content moderation; EU legislation.

Науковий керівник: к.ю.н. доцент Чанишев Р.І.

ЗМІСТ

Секція 1. АЛГОРИТМІЧНІ ТА ТЕХНІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ... 10

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ У СОЦІАЛЬНИХ МЕРЕЖАХ: ВИКЛИКИ ТА ЗАГРОЗИ СУЧАСНОГО ЕТАПУ 10
Дикий Олег

A REVIEW ON MANY-VALUED LOGIC: A NOVEL PARADIGM FOR INFORMATION SECURITY 12
Aboobacker P

МЕТОДИ ТА РИЗИКИ ПОБУДОВИ СИСТЕМ З END-TO-END ШИФРУВАННЯМ 15
Вінковська Ірина
Чебаненко Олег

A 10-BIT S-BOX GENERATED BY FEISTEL CONSTRUCTION FROM CELLULAR AUTOMATA 217
Thomas Prévost
Bruno Martin

СИСТЕМИ РАНЖУВАННЯ ТА АНАЛІЗУ ІНФОРМАЦІЇ ПРИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ 26
Кухаренко Сергій
Сидорчук Владислав

БЕЗПЕКА ANDROID-ЗАСТОСУНКІВ НА KOTLIN ТА JETPACK COMPOSE 29
Манаков Сергій

КОНЦЕПЦІЯ ТА РОЗГОРТАННЯ ВИСОКОІНТЕРАКТИВНОГО ХАНІПОТУ НА НА ОСНОВІ ЕМУЛЯЦІЇ ЛЕГІТИМНОГО ВЕБСЕРВЕРА (NGINX) 29
Бойко Віктор

МІЖНАБОРНЕ ТЕСТУВАННЯ МЕТОДУ KNN+TF-IDF У ЗАДАЧІ ВИЯВЛЕННЯ ІН'ЄКЦІЙНИХ АТАК У ВЕБ-ЗАПИТАХ 34
Коробейнікова Тетяна
Кравчук Назар

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ СУЧАСНОГО РИНКУ ВІДЕОІГОР 37
Куклінова Тетяна
Гулієва Анастасія

ВИКОРИСТАННЯ OPENDATA UKRAINE В ЦІЛЯХ OSINT 40
Бойко Віктор
Дручик Софія

ЛОКАЛЬНИЙ МЕНЕДЖЕР ПАРОЛІВ ІЗ ГЕНЕРУВАННЯМ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ 40
Тимошенко Лідія
Вакуліна Сана
Волобуєва Ірина

СУЧАСНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІНТЕЛЕКТУАЛЬНИХ ЖИТЛОВИХ СИСТЕМАХ 47
Неділенко Валерій

МЕТОД ФАКТОРИЗАЦІЇ ВЕЛИКИХ ЧИСЕЛ 49
Тимошенко Лідія
Алєксєєва Софія

НОВІТНІ НАПРЯМИ РОЗВИТКУ СУЧАСНИХ БАЗ ДАНИХ 51
Щербина Ю. В.

ПРОБЛЕМА БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ У CRM-СИСТЕМАХ (НА ПРИКЛАДІ SALESFORCE) 56
Бойко Віктор
Перепелиця Марія

ЗАХИСТ ІГРОВИХ РЕСУРСІВ У СУЧАСНИХ ВІДЕОІГРАХ: КОНЦЕПЦІЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ В ГРІ «HONEY & MOLD» 59
Дяченко Аріна
Соколов Артем

АЛГОРИТМІЧНІ ПІДХОДИ ДО ПІДТВЕРДЖЕННЯ АВТОРСТВА ТА ЦІЛІСНОСТІ МУЛЬТИМЕДІЙНИХ ДАНИХ 62
Овчинников Микола

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ КІБЕРБЕЗПЕКИ В ОНЛАЙН ТА ОФЛАЙН ІГРАХ 65
Скідан Владислав

СИСТЕМА ВИЯВЛЕННЯ ВИТОКІВ ПЕРСОНАЛЬНИХ ДАНИХ 67
Бойко Віктор
Вередін Діана

РОЗРОБКА ІНСТРУМЕНТУ АНАЛІЗУ ТА ОЦІНКИ БЕЗПЕКИ WI-FI МЕРЕЖ В УМОВАХ СУЧАСНИХ КІБЕРЗАГРОЗ 670
Бабенко Кирило

ГЕНЕРАЦІЯ ДИНАМІЧНИХ S-БЛОКІВ (F-БЛОКІВ) НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ 74
Роговий Іван

СТВОРЕННЯ ФІШИНГОВОГО СЦЕНАРІЮ ТА АНАЛІЗ РЕАКЦІЇ КОРИСТУВАЧІВ 77
Тинкевич Дана

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАХИСТУ ЛОГІВ 81
Бойко Віктор
Вуль Анастасія

ПРОВЕДЕННЯ SQL-ІН'ЄКЦІЇ З ВИКОРИСТАННЯМ SQLMAP 84
Клевець Михайло

СИСТЕМНИЙ АНАЛІЗ ТА ОЦІНКА РИЗИКІВ ВРАЗЛИВОСТІ ІОТ-ПРИСТРОЇВ 83
Гура Володимир
Мурзін Олександр

ПРОЦЕДУРА ШИФРУВАННЯ З ВИКОРИСТАННЯМ ДВОМІРНИХ КЛІТИННИХ АВТОМАТІВ 94
Бойко Віктор
Сутурін Євгеній

Секція 2. ШТУЧНИЙ ІНТЕЛЕКТ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ 96

АЛГОРИТМИ МАШИННОГО НАВЧАННЯ У КОМП'ЮТЕРНОМУ ЗОРІ 96
Логінова Наталія

ШТУЧНИЙ ІНТЕЛЕКТ І МАШИННЕ НАВЧАННЯ У КІБЕРБЕЗПЕЦІ 100
Воронянський Володимир
Шкавро Наталія

ВИКОРИСТАННЯ ЧАТ-БОТІВ З LLM-МОДЕЛЯМИ У ВИВЧЕННІ МОВ 103
Трофименко Олена
Алі Амір

ІНТЕГРАЦІЯ ФУНКЦІОНАЛУ ЧАТ-БОТІВ У СИСТЕМИ МОНІТОРИНГУ ВЕБ-СЕРВЕРІВ ДЛЯ ЗМЕНШЕННЯ ЧАСУ РЕАКЦІЇ НА КІБЕРЗАГРОЗИ 106
Бойко Віктор
Наконечний Микита

СУВЕРЕННІ ХМАРНІ ІНФРАСТРУКТУРИ ЯК ОСНОВА ЦИФРОВОГО СУВЕРЕНІТЕТУ 109
Чанишев Рашид

ГРАФОВІ МОДЕЛІ ДЛЯ ВАЛІДАЦІЇ ВРАЗЛИВОСТЕЙ 112
Денисюк Владислав

AI-ПІДСИЛЕНА ВЕРИФІКАЦІЯ АВТОРСТВА МУЛЬТИМЕДІЙНИХ ДАНИХ В УМОВАХ ГЕНЕРАТИВНОГО ШІ 115
Овчинников Микола

САМОВДОСКОНАЛЮВАНІ ВІРУСИ ШТУЧНОГО ІНТЕЛЕКТУ: РИЗИКИ, ВИЯВЛЕННЯ ТА МЕТОДИ ПРОТИДІЇ 117
Лавренко Дмитро

МАШИННЕ НАВЧАННЯ У ПЕРЕВІРЦІ ПРОГРАМНИХ КОДІВ: ЕФЕКТИВНІСТЬ АЛГОРИТМУ RANDOM FOREST 120
Григор'єв Олександр

ІНТЕРНЕТ РЕЧЕЙ (IOT) ЯК ІНСТРУМЕНТ БІЗНЕС-МЕНЕДЖМЕНТУ 123
Літовченко Данило

МЕТОДИ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЗНАЧЕННЯ СТИЛІВ НАВЧАННЯ 126
Дашдаміров Гліб

КОНТРОЛЬ ЦІЛІСНОСТІ БАЗИ ДАНИХ ЗА ДОПОМОГОЮ БЛОКЧЕЙНІВ 128
Бойко Віктор
Панчук Ганна

ОГЛЯД ЕВОЛЮЦІЇ АРХІТЕКТУРИ ІГРОВИХ РУШІЇВ 1328
Толокнов Анатолій

БЛОКЧЕЙН-ТЕХНОЛОГІЇ В ЗАБЕЗПЕЧЕННІ ЦІЛІСНОСТІ ДАНИХ 136
Соловйов Артем

ІНФОРМАЦІЙНА ГЕОМЕТРІЯ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ТОЧНОСТІ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ 139
Чепурна Олена
Черевко Євген

ВРАХУВАННЯ ЕНЕРГОЕФЕКТИВНОСТІ ТА РОБАСТНОСТІ В МОДЕЛЯХ СИСТЕМ КІБЕРБЕЗПЕКИ 141
Юсипів Андрій

ІДІОМА RAII ЯК ЕВОЛЮЦІЙНА ВІДПОВІДЬ НА ПРОБЛЕМИ РУЧНОГО УПРАВЛІННЯ ПАМ'ЯТТЮ В C++ 146
Д'якова Ксенія

ВИКОРИСТАННЯ МУЛЬТИМЕДІЙНИХ ТЕХНОЛОГІЙ У СТВОРЕННІ СУЧАСНИХ ІГРОВИХ ЗАСТОСУНКІВ 149
Задерейко Олександр
Корчовий Михайло

АНАЛІЗ СУЧАСНОГО СТАНУ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 152
Світличний Дмитро

АНАЛІЗ ІНСТРУМЕНТІВ ТА ПЛАТФОРМ ДЛЯ ТРЕКІНГУ ЕКСПЕРИМЕНТІВ 156
Савенко Михайло

АРХІТЕКТУРНІ ТА АЛГОРИТМІЧНІ ВИКЛИКИ НАВЧАННЯ ASR-МОДЕЛЕЙ ДЛЯ РОЗПІЗНАВАННЯ УКРАЇНСЬКОГО МОВЛЕННЯ 158
Антіпіна Надія

АРХІТЕКТУРА ТА ОСНОВНІ КОМПОНЕНТИ AUTOML-СИСТЕМ 161
Лобода Юлія
Дерев'ягін Владислав

ІНТЕЛЕКТУАЛЬНИЙ ЧАТ-БОТ ДЛЯ НАВЧАННЯ АНГЛІЙСЬКОЇ МОВИ: АРХІТЕКТУРА ТА ФУНКЦІОНАЛЬНА МОДЕЛЬ 165
Трофименко Олена
Безродний Микола

РОЗРОБКА ОСВІТНЬОГО МОДУЛЯ «ОРГАНІЗАЦІЯ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ ЗА ІНТЕРФЕЙСОМ OPENMP» 167
Чикунов Павло
Богун Валентин

ДОСЛІДЖЕННЯ СПЕКТРАЛЬНОЇ ДЕГРАДАЦІЇ СЕЛЕКТИВНОСТІ БІНАРНИХ КОДОВИХ СЛІВ ПРИ МАСШТАБУВАННІ 171
Баландіна Наталія

МЕТОДИ АНАЛІЗУ ДАНИХ У ПРОГНОЗУВАННІ ПОПИТУ НА ТОВАРИ ЕКТРОННОЇ КОМЕРЦІЇ 176
Лобода Юлія
Дроздов Богдан

МУЛЬТИМЕДІЙНІ СИСТЕМИ ДЛЯ МОНІТОРИНГУ ТА АНАЛІЗУ КОНТЕНТУ ВІДЕОПЛАТФОРМ 183
Задерейко Олександр
Барбенягре Валерія

АНАЛІЗ СУЧАСНИХ МЕХАНІЗМІВ ЗАХИСТУ ВІД АТАК НА ВИЯВЛЕННЯ НАЛЕЖНОСТІ 173
Хоменко Ігор

ВИЯВЛЕННЯ НЕТИПОВИХ ПОДІЙ У СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ 167
Чикунов Павло
Флюнт Владислав

АНАЛІЗ ТА РЕДИЗАЙН МОБІЛЬНОГО ЗАСТОСУНКУ НА ОСНОВІ UX-ДОСЛІДЖЕННЯ ТА ПРОТОТИПУВАННЯ 185
Селютін В'ячеслав

ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ LOW-CODE ПЛАТФОРМ ДЛЯ ПРИСКОРЕННЯ РОЗРОБКИ КОРПОРАТИВНИХ ЗАСТОСУНКІВ 198
Гура Володимир
Дацко Іван

АРХІТЕКТУРНІ ТА АЛГОРИТМІЧНІ ВИКЛИКИ КІБЕРБЕЗПЕКИ У ПРОГНОСТИЧНИХ AR-СИСТЕМАХ НА ОСНОВІ МУЛЬТИМОДАЛЬНОГО АНАЛІЗУ 167
Чикунов Павло
Пучков Владислав

АНАЛІЗ СУЧАСНИХ ІГРОВИХ РУШІЇВ GAMEDEV 167
Кутас Олександр

СУЧАСНІ МЕТОДИ АНАЛІЗУ ДАНИХ ДЛЯ ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ 211
Гура Володимир
Гандзій Ілля

РОЗРОБКА ОСВІТНЬОГО МОДУЛЯ «РЕФАКТОРИНГ ЗАДАЧ УЗАГАЛЬНЕННЯ ОБЄ'КТІВ» 167
Чикунов Павло
Колеснік Євгеній

Секція 3. УПРАВЛІНСЬКІ, СОЦІАЛЬНІ ТА ПСИХОЛОГІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ.....2211

ПЕРСПЕКТИВИ СТВОРЕННЯ КЛАСТЕРУ КІБЕРБЕЗПЕКИ В УКРАЇНІ.....213
Горбаченко Станіслав
Саврацький Олександр

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ТОКСИЧНОГО КОНТЕНТУ ПРИ СПІЛКУВАННІ УКРАЇНСЬКОЮ МОВОЮ 218
Гура Володимир
Касян Павло

ГЕНЕЗИС РОЗВИТКУ 3D-ТЕХНОЛОГІЙ У МОДЕЛЮВАННІ ТА АНІМАЦІЇ 221
Задерейко Олександр
Тимофєєв Михайло

ОСОБЛИВОСТІ ЗАХОДІВ КІБЕРБЕЗПЕКИ У РЕСТОРАННІЙ СФЕРІ.....224
Разінкін Нікіта
Нгуен Фиок Бао Шон

СИСТЕМНИЙ АНАЛІЗ ТА ОПТИМІЗАЦІЯ ЕФЕКТИВНОСТІ ВЕБПОРТАЛУ НА ОСНОВІ ПОВЕДІНКИ КОРИСТУВАЧА.....228
Куклінова Софія

ANALYSIS AND MODELING OF THE PLAYER'S EMOTIONAL STATES IN ADAPTIVE GAME DESIGN SYSTEMS 230
Chepurna Olena
Shliakhtytskyi Dmytro

ДОСЛІДЖЕННЯ МЕТОДІВ АДАПТАЦІЇ ІНТЕРФЕЙСІВ ДЛЯ КОРИСТУВАЧІВ З КОГНІТИВНИМИ ПОРУШЕННЯМИ.....2360
Гура Володимир
Вдовін Олександр

КОМУНІКАЦІЙНІ СТРАТЕГІЇ ПРОТИДІЇ РЕПОСТАМ І «ДЗЕРКАЛАМ» МУЛЬТИМЕДІЙНОГО КОНТЕНТУ: ВЗАЄМОДІЯ З ПЛАТФОРМАМИ ТА СПІЛЬНОТАМИ 239
Овчинников Микола

ПЛАТФОРМЕНА ЕКОНОМІКА: МОЖЛИВОСТІ ТА ВИКЛИКИ.....241
Маріна Аліна

НМІ ЯК ЧИННИК ЦИФРОВОЇ ЕВОЛЮЦІЇ УПРАВЛІНСЬКИХ ПРАКТИК 245
Кочубинська Юлія

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОДУКТИВНОСТІ ДЕКЛАРАТИВНОГО ТА ІМПЕРАТИВНОГО ПІДХОДІВ ДО ПОБУДОВИ КОРИСТУВАЦЬКИХ ІНТЕРФЕЙСІВ МОБІЛЬНИХ ЗАСТОСУНКІВ.....2475
Земан Артур

COMPETITION AND MARKETS AUTHORITY (CMA): УПРАВЛІННЯ КОНКУРЕНЦІЄЮ В ЕПОХУ ЦИФРОВИХ РИНКІВ 251
Власюк Олександра

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації 251

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ 255
Задерейко Олександр
Іванов Володимир

АНАЛІЗ МЕТОДІВ ВИЛУЧЕННЯ КЛЮЧОВОЇ ІНФОРМАЦІЇ З ЮРИДИЧНИХ ТЕКСТІВ 262
Гура Володимир
Курчук Роман

ЄВРОПЕЙСЬКИЙ ЗАГАЛЬНИЙ РЕГЛАМЕНТ ЗАХИСТУ ДАНИХ (GDPR): НАПРЯМИ ДІЇ, ВПЛИВ І ВИКЛИКИ 265
Шевчук Марія

ЛІЦЕНЗУВАННЯ ТА УПРАВЛІННЯ ПРАВАМИ НА ЦИФРОВИЙ МУЛЬТИМЕДІЙНИЙ КОНТЕНТ: ІНТЕГРАЦІЯ ТЕХНІЧНИХ ЗАСОБІВ КОНТРОЛЮ У ПРАВОВІ ПРОЦЕДУРИ 268
Овчинников Микола

СТРАТЕГІЧНІ ТА ТЕХНІЧНІ ЗАСАДИ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА 271
Костіна Олександра

ШТУЧНИЙ ІНТЕЛЕКТ І ФІНАНСОВА СТАБІЛЬНІСТЬ: КЛЮЧОВІ ВИСНОВКИ КОМІТЕТУ З ФІНАНСОВОЇ ПОЛІТИКИ ВЕЛИКОЇ БРИТАНІЇ 274
Мовчан Анастасія

AEVA 2018: РЕГУЛЯТОРНІ ЗАСАДИ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ В ТРАНСПОРТНУ ІНФРАСТРУКТУРУ ВЕЛИКОЇ БРИТАНІЇ 277
Лозовій Вероніка

ПРАВОВІ ІНСТРУМЕНТИ ЄС У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ РИНКУ МОБІЛЬНИХ ДОДАТКІВ 277
Волонтирець Анастасія

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ ТА ПРАКТИКА

МАТЕРІАЛИ
VI МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ

28 листопада 2025 року
м. Одеса

Відповідальній редактор: О.В. Дикий

Дизайн та верстка:
М.Ю. Овчинников

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ ТА ПРАКТИКА

28 листопада 2025 року, м. Одеса