ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

За загальною редакцією ***С. В. Ківалова***

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск ***М. Р. Аракелян***

ISBN 978-617-8430-61-0

СЕКЦІЯ 24. КОГНІТИВНО-ПРАГМАТИЧНІ ДОСЛІДЖЕННЯ ДИСКУРСУ, ТЕОРІЯ ТА ПРАКТИКА ПЕРЕКЛАДУ В АСПЕКТІ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ

шляхом інтеграції з мережевими датчиками та використання трансформерів для обробки складніших часових рядів із довжиною понад 50 кроків. Цей підхід може стати основою для створення проактивних систем кіберзахисту, здатних прогнозувати та запобігати загрозам у реальному часі з точністю прогнозування до 98%.

Список використаних джерел:

1. Changala R., Kayalvili S., Farooq M., Rao M., Vuda T., Rao S. Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity. *2024 International Conference on Data Science and Network Security (ICDSNS).* 2024. P. 1–6. DOI: 10.1109/ICDSNS62112.2024.10690857

2. Lim W., Yong K. S. C., Lau B. T., Tan C. C. L. Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. *Computers & Security.* 2024. Vol. 139. 103733. 11 p. URL: https://doi.org/10.1016/j.cose.2024.103733.

Ключові слов: штучний інтелект, кібербезпека, методи і системи штучного інтелекту, Python, нейронні мережі.

Keywords: artificial intelligence, cybersecurity, artificial intelligence methods and systems, Python, neural networks.

Скідан Владислав Сергійович
Національний університет «Одеська юридична академія»,
аспірант кафедри кібербезпеки

ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ГЕЙМІФІКАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ

Гейміфікація навчального процесу зазвичай реалізується через спеціалізовані платформи, мобільні додатки чи веб-сервіси, які збирають великий обсяг даних про користувачів. Ці дані включають не лише базову інформацію, таку як ім'я, вік чи навчальний заклад, а й деталізовані профілі поведінки: час, витрачений на завдання, рівень успішності, переваги в ігрових механіках, а подекуди навіть геолокацію чи взаємодію з іншими учасниками. Наприклад, платформа Kahoot!, яка широко використовується в школах по всьому світу, дозволяє вчителям створювати інтерактивні вікторини, а учням – брати участь у них у реальному часі. Хоча це сприяє залученості, сервери платформи зберігають дані про кожну сесію, що потенційно може стати мішенню для кібератак. Аналогічно Duolingo, додаток для вивчення мов із гейміфікованим підходом, відстежує прогрес користувачів, їхні помилки та навіть частоту використання, що вимагає надійного шифрування та захисту від несанкціонованого доступу [1].

Одним із головних ризиків є недостатня обізнаність розробників гейміфікованих систем і педагогів щодо стандартів кібербезпеки. Багато платформ ство-

рюються з акцентом на функціональність і привабливий дизайн, тоді як аспекти безпеки часто відходять на другий план. У 2018 році, наприклад, стало відомо про витік даних із платформи ClassDojo, яка використовує елементи гейміфікації для управління поведінкою учнів у класі. Зловмисники отримали доступ до інформації про мільйони учнів і вчителів через вразливість у системі аутентифікації [2]. Цей випадок підкреслив, наскільки важливо впроваджувати двофакторну аутентифікацію, регулярні оновлення програмного забезпечення та аудит безпеки для подібних інструментів.

Ще однією проблемою є використання гейміфікації в умовах недостатнього регулювання. У країнах Європейського Союзу, де діє Загальний регламент захисту даних (GDPR), розробники зобов'язані забезпечувати прозорість обробки даних, отримувати згоду користувачів і гарантувати їхнє право на видалення інформації [3]. Проте в інших регіонах, де подібні закони менш суворі, компанії можуть накопичувати дані без належного інформування учнів чи їхніх батьків. Наприклад, у США платформи на кшталт Edmodo, що застосовують гейміфікацію для домашніх завдань, неодноразово критикувалися за передачу даних третім сторонам для маркетингових цілей, що порушує етичні норми використання інформації в освіті.

Технічні аспекти захисту інформації також відіграють вирішальну роль. Гейміфіковані системи часто інтегруються з хмарними сервісами, що підвищує ризик атак типу "людина посередині" або фішингу. У 2020 році дослідники виявили вразливість у платформі Quizizz, яка, подібно до Kahoot!, використовується для інтерактивних тестів. Зловмисники могли перехоплювати не зашифровані запити, отримуючи доступ до результатів учнів і навіть вмісту завдань [4]. Це свідчить про необхідність використання протоколів HTTPS, шифрування даних у транзиті та на стороні сервера, а також регулярного тестування на проникнення.

Соціальний аспект проблеми не менш важливий. Гейміфікація часто передбачає конкурентні елементи, такі як рейтинги чи таблиці лідерів, що може спонукати учнів ділитися персональною інформацією заради досягнення вищих позицій. Наприклад, у системі Classcraft, яка перетворює навчання на рольову гру, учасники можуть створювати профілі з аватарами та описами, що іноді включають реальні фотографії чи особисті деталі. Без належного контролю це створює ризик кібербулінгу або крадіжки ідентичності [5]. Освітні заклади, які впроваджують такі інструменти, повинні забезпечувати чіткі інструкції щодо безпечної поведінки в цифровому середовищі та обмежувати обсяг відкритої інформації.

Для оцінки ризиків і методів їхнього мінімізації корисно розглянути структуру типових загроз і відповідних заходів захисту. Таблиця 1 систематизує основні аспекти інформаційної безпеки в контексті гейміфікації навчального процесу, базуючись на реальних прикладах і сучасних підходах до кібербезпеки.

Таблиця 1. Основні аспекти інформаційної безпеки

Аспект	Опис загрози	Приклад із реального досвіду	Заходи захисту
Збір персональних даних	Витік інформації через недостатнє шифрування чи слабкі паролі	Витік даних із ClassDojo у 2018 році	Шифрування AES-256, двофакторна аутентифікація, політика сильних паролів
Хмарні сервіси	Перехоплення даних через незахищені з'єднання	Вразливість у Quizizz у 2020 році	Використання HTTPS, шифрування в транзиті, регулярне тестування на проникнення
Регуляторна відповідність	Передача даних третім сторонам без згоди користувачів	Критика Edmodo за маркетингові угоди в США	Дотримання GDPR, прозорі угоди з користувачами, право на видалення даних
Соціальні ризики	Використання особистих даних у відкритих рейтингах чи профілях	Потенційні проблеми в Classcraft із аватарами	Обмеження відкритої інформації, навчання цифровій грамотності, модерація вмісту
Технічні вразливості	Атаки на сервери через застаріле програмне забезпечення	Загрози для платформ із відкритим кодом	Регулярні оновлення, аудит безпеки, використання захищених API

Захист інформації при використанні гейміфікації навчального процесу вимагає комплексного підходу, який поєднує технічні, правові та педагогічні заходи. Розробники платформ повинні приділяти увагу не лише ігровій механіці, а й створенню безпечного середовища, де дані учнів і вчителів перебувають під надійним захистом. Освітні заклади, зі свого боку, мають впроваджувати політику цифрової безпеки, навчати учнів і персонал основам кібергігієни та співпрацювати з постачальниками технологій для забезпечення відповідності стандартам. Тільки за таких умов гейміфікація зможе реалізувати свій потенціал як інноваційний інструмент навчання, не ставлячи під загрозу конфіденційність і безпеку її учасників. Цей баланс між інноваціями та захистом є визначальним для майбутнього цифрової освіти.

Список використаних джерел:

1. Чижикова І. Розвиток навчальної автономії студентів в умовах гейміфікації навчального процесу у ЗВО. *Освіта. Інноватика. Практика.* 2023. № 11(2). С. 54-59.

2. Матківський М. П., Тарас Т. М., Лучкевич Є. Р. Роль гейміфікації у покращенні мотивації та навчальних результатів учнів середньої школи в умовах цифрової трансформації освіти в Україні. *Педагогічна Академія: наукові записки.* 2025. № 14. URL: https://pedagogical-academy.com/index.php/journal/article/view/571/455 (дата звернення: 01.04.2025).

3. Годлевська К. Особливості технологічного аспекту ефективної реалізації змішаного навчання в сучасних умовах сьогодення. *UNESCO Chair Journal Lifelong Professional Education in the XXI Century.* 2024. № 2(10). С. 46-56.

4. Ткаченко К. О., Ісаченко Б. О. Використання гейміфікації в інтелектуальних навчальних системах та їх вебдизайні. водний транспорт. Водний транспорт. 2023. № 2(38). С. 299-311.

5. Козуб Г. О., Шинкаренко Я. М., Козуб В. Ю. Гейміфікація в освіті: інтеграція Classcraft в навчальний процес. *Педагогічна Академія: наукові записки*. 2024. № 7. https://doi.org/10.57125/pedacademy.2024.06.29.02

Ключові слова: гейміфікації, захист інформації, безпека, освітня програма, інструменти.
Keywords: gamification, information protection, security, educational program, tools.

Поворознюк Олексій Олегович
Національний університет «Одеська юридична академія»,
аспірант кафедри кібербезпеки

МЕТОДИ ЗАХИСТУ МУЛЬТИМЕДІЙНИХ ДАНИХ ПІД ЧАС ВІЙНИ

У сучасних збройних конфліктах між Україною та росією інформація розповсюджується миттєво, а візуальні та аудіовізуальні матеріали формують сприйняття війни як всередині нашої країни, так і за її межами. Фотографії, відеозаписи, аудіофайли та текстові повідомлення можуть містити критично важливу інформацію, яка, у разі потрапляння до рук противника, здатна призвести до катастрофічних наслідків. Саме тому питання захисту мультимедійних даних набуває особливої актуальності, адже війна ведеться не лише на полі бою, а й у кіберпросторі [1].

Сучасні технології дозволяють противнику перехоплювати та аналізувати цифрові матеріали, а тому важливо використовувати методи шифрування та анонімізації, які ускладнюють витік інформації. Зокрема, військові, волонтери, журналісти та цивільні особи повинні враховувати ризики, пов'язані з використанням відкритих каналів передачі даних, таких як месенджери чи соціальні мережі. Недостатній рівень захисту може спричинити викриття позицій військових, розкриття особистих даних людей, які перебувають у зоні бойових дій, або навіть створення дезінформаційних кампаній на основі викрадених матеріалів.

Фальсифікація зображень і відео, поширення дезінформації та фабрикація доказів є частиною стратегії ворога, спрямованої на дестабілізацію суспільства.