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».

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».

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)

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?l 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

ЗМІСТ