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)

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

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.

ЗМІСТ