ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТУ ІМЕНІ С.П.КОРОЛЬОВА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

здобувача вищої освіти ступеня «бакалавр» заочної форми навчання
за спеціальністю «Кібербезпека»

Тема: «АНАЛІЗ ЕФЕКТИВНОСТІ ПРОТОКОЛІВ Wi-Fi У ЗАБЕЗПЕЧЕННІ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ»

Виконавець: Віталій ВОЛКОВ

м. Житомир

2026

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох основних розділів, висновків та переліку джерел посилань. Обсяг основного тексту кваліфікаційної роботи становить 50 сторінок; робота містить 10 рисунків і 9 таблиць; використано 21 джерело. Загальний обсяг роботи становить 73 сторінок.

Мета роботи: провести аналіз ефективності протоколів Wi-Fi у забезпеченні захисту бездротових мереж, здійснити практичне тестування захищеності мереж при використанні протоколів WEP та WPA2 та сформулювати практичні рекомендації щодо їх застосування.

Об'єкт дослідження: бездротові мережі стандарту Wi-Fi та їх захист від несанкціонованого доступу.

Предмет дослідження: протоколи безпеки Wi-Fi (WEP, WPA, WPA2, WPA3) та показники їхньої ефективності у забезпеченні захисту бездротових мереж.

Методи дослідження: аналіз науково-технічної літератури та нормативних документів у сфері кібербезпеки; порівняльний аналіз технічних характеристик протоколів; багатокритеріальне оцінювання із застосуванням методу зваженої суми; практичне тестування захищеності бездротових мереж з використанням програмних засобів CommView for Wi-Fi, Aircrack-ng та Wireshark; системний підхід до аналізу механізмів захисту бездротових мереж.

Отримані результати: проведено теоретичний аналіз та порівняльне оцінювання ефективності протоколів WEP, WPA, WPA2 та WPA3 за критеріями стійкості (вага 0,45), продуктивності (вага 0,30) та практичної реалізованості (вага 0,25). Встановлено ієрархію інтегральної ефективності: WPA3 (9,2/10) > WPA2 (7,8/10) > WPA (6,2/10) > WEP (4,9/10). Практичними експериментами підтверджено: ключ мережі з протоколом WEP відновлено за 9 хв 47 с; пароль мережі WPA2 зі слабкою парольною фразою знайдено за 16 хв 25 с; захищену конфігурацію WPA2 з AES-CCMP, складним паролем і вимкненим WPS у межах перевірених сценаріїв скомпрометувати не вдалося.

Рекомендації: для нових розгортань Wi-Fi мереж рекомендується використання протоколу WPA3 або режиму сумісності WPA2/WPA3. Для корпоративних мереж - WPA3-Enterprise з методом автентифікації EAP-TLS. Незалежно від обраного протоколу критично важливо використовувати паролі довжиною не менше 20 символів, вимикати WPS та регулярно оновлювати прошивки точок доступу. Результати роботи можуть бути використані при проектуванні та модернізації систем захисту бездротових мереж.

Ключові слова: протоколи безпеки Wi-Fi, WEP, WPA, WPA2, WPA3, захист бездротових мереж, AES, CCMP, SAE, Aircrack-ng, криптографічний захист, автентифікація, шифрування.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

AAA	–	Authentication, Authorization, Accounting (автентифікація, авторизація, облік);
AES	–	Advanced Encryption Standard (розширений стандарт шифрування);
AID	–	Association Identifier (ідентифікатор асоціації);
ANonce	–	Authenticator Nonce (випадкове значення автентифікатора);
AP	–	Access Point (точка доступу);
BSSID	–	Basic Service Set Identifier (ідентифікатор базового набору послуг);
CBC-MAC	–	Cipher Block Chaining Message Authentication Code;
CCMP	–	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol;
CIA	–	Confidentiality, Integrity, Availability (конфіденційність, цілісність, доступність);
CPU	–	Central Processing Unit (центральний процесор);
CRC	–	Cyclic Redundancy Check (циклічна надлишкова перевірка);
CTR	–	Counter Mode (режим лічильника);
DoS	–	Denial of Service (відмова в обслуговуванні);
DPAPI	–	Data Protection API;
EAP	–	Extensible Authentication Protocol (розширюваний протокол автентифікації);
EAPOL	–	EAP over LAN;
EAP-FAST	–	EAP Flexible Authentication via Secure Tunneling;
EAP-PEAP	–	Protected Extensible Authentication Protocol;
EAP-TLS	–	EAP Transport Layer Security;
EAP-TTLS	–	EAP Tunneled Transport Layer Security;
FCS	–	Frame Check Sequence (послідовність перевірки кадру);
GCMP	–	Galois/Counter Mode Protocol;
GCM	–	Galois/Counter Mode;
GHASH	–	Galois Hash;
GTK	–	Group Temporal Key (груповий тимчасовий ключ);
GUI	–	Graphical User Interface (графічний інтерфейс користувача);
HMAC	–	Hash-based Message Authentication Code;
IDS	–	Intrusion Detection System (система виявлення вторгнень);
IEEE	–	Institute of Electrical and Electronics Engineers;
IPS	–	Intrusion Prevention System (система запобігання вторгненням);

IV – Initialization Vector (вектор ініціалізації);
KCK – Key Confirmation Key (ключ підтвердження ключів);
KEK – Key Encryption Key (ключ шифрування ключів);
MAC – Message Authentication Code / Medium Access Control;
MFP – Management Frame Protection (захист управляючих фреймів);
MIC – Message Integrity Code (код цілісності повідомлення);
MitM – Man-in-the-Middle (атака «людина посередині»);
MPDU – MAC Protocol Data Unit;
NIST – National Institute of Standards and Technology;
ОС – Операційна система
OWE – Opportunistic Wireless Encryption;
PBKDF2 – Password-Based Key Derivation Function 2;
PMK – Pairwise Master Key (парний головний ключ);
PMKID – Pairwise Master Key Identifier;
PN – Packet Number (порядковий номер пакета);
PSK – Pre-Shared Key (попередньо розповсюджений ключ);
PTK – Pairwise Transient Key (парний тимчасовий ключ);
RADIUS – Remote Authentication Dial-In User Service;
RC4 – Rivest Cipher 4;
RSA – Rivest-Shamir-Adleman (алгоритм шифрування);
SAE – Simultaneous Authentication of Equals;
SHA – Secure Hash Algorithm;
SNonce – Supplicant Nonce (випадкове значення суплікант);
SSID – Service Set Identifier (ідентифікатор набору послуг);
с – секунди;
СУІБ – Система управління інформаційною безпекою;
TK – Temporal Key (тимчасовий ключ);
TKIP – Temporal Key Integrity Protocol;
TSC – TKIP Sequence Counter;
VPN – Virtual Private Network (віртуальна приватна мережа);
VLAN – Virtual Local Area Network (віртуальна локальна мережа);
WEP – Wired Equivalent Privacy;
Wi-Fi – Wireless Fidelity;
WIDS – Wireless Intrusion Detection System;
WIPS – Wireless Intrusion Prevention System;
WPA – Wi-Fi Protected Access;
WPA2 – Wi-Fi Protected Access 2;
WPA3 – Wi-Fi Protected Access 3;
WPS – Wi-Fi Protected Setup;
хв – хвилини;
XOR – eXclusive OR (виключне або).

ВСТУП

Бездротові мережі стандарту Wi-Fi стали невід'ємною складовою сучасної інформаційної інфраструктури - від домашніх мереж до корпоративних середовищ та об'єктів критичного значення. За даними Wi-Fi Alliance, станом на 2024 рік у світі функціонує понад 20 мільярдів Wi-Fi пристроїв, що підкреслює масштаби явища. Водночас відкрита природа радіосередовища робить бездротові мережі принципово вразливішими порівняно з провідними: будь-який пристрій у зоні дії сигналу здатний перехоплювати трафік або здійснювати спроби несанкціонованого доступу.

Забезпечення захисту бездротових мереж здійснюється передусім засобами протоколів безпеки Wi-Fi, які пройшли тривалий еволюційний шлях: від WEP (1997) через WPA та WPA2 до сучасного WPA3 (2018). Кожне покоління протоколів усувало вразливості попередника, проте на практиці значна частина розгорнутих мереж досі використовує застарілі або некоректно налаштовані протоколи. Показово, що навіть криптографічно стійкий WPA2 залишається вразливим при слабкій конфігурації - зокрема, при використанні простих паролів. Крім того, загрози не стоять на місці: атаки KRACK (2017), Dragonblood (2019), PMKID та методи перебору словника паролів демонструють, що проблема захисту бездротових мереж не втрачає актуальності.

В умовах зростання кіберзагроз, у тому числі в контексті забезпечення кібербезпеки України, об'єктивна оцінка ефективності наявних протоколів Wi-Fi та вироблення практичних рекомендацій щодо їх застосування є важливим прикладним завданням. Це підтверджується вимогами міжнародних стандартів ISO/IEC 27001, 27002, рекомендацій NIST SP 800-153, а також національного законодавства у сфері кібербезпеки.

Мета роботи - провести аналіз ефективності протоколів Wi-Fi у забезпеченні захисту бездротових мереж, виконати порівняльне оцінювання

протоколів WEP, WPA, WPA2 та WPA3 і сформулювати практичні рекомендації щодо їх застосування.

Об’єкт дослідження - бездротові мережі стандарту Wi-Fi та механізми їх захисту від несанкціонованого доступу.

Предмет дослідження - протоколи безпеки Wi-Fi WEP, WPA, WPA2, WPA3 та показники їх ефективності у забезпеченні захисту бездротових мереж.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1) розкрити сутність протоколів безпеки Wi-Fi та механізмів криптографічного захисту;

2) проаналізувати особливості автентифікації, шифрування та управління ключами у WEP, WPA, WPA2 та WPA3;

3) визначити основні загрози безпеці бездротових мереж;

4) провести порівняльне оцінювання ефективності протоколів за критеріями стійкості, продуктивності та практичної реалізованості;

5) виконати практичне тестування типових конфігурацій бездротових мереж;

6) сформулювати рекомендації щодо вибору та налаштування протоколів захисту Wi-Fi.

Методи дослідження: аналіз науково-технічної літератури та нормативних документів; порівняльний аналіз характеристик протоколів; багатокритеріальне оцінювання методом зваженої суми; практичне тестування у контрольованому лабораторному середовищі; системний підхід до аналізу механізмів захисту бездротових мереж.

РОЗДІЛ 1
ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ АНАЛІЗУ ЕФЕКТИВНОСТІ ПРОТОКОЛІВ WI-FI У ЗАБЕЗПЕЧЕННІ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

1.1 Сутність поняття «протокол безпеки Wi-Fi» та основи криптографічного захисту

Бездротові мережі Wi-Fi стали важливою складовою сучасної інформаційної інфраструктури. Вони використовуються у домашніх мережах, корпоративному середовищі та на об’єктах критичного значення. Зростання масштабів їх застосування посилює вимоги до захисту, оскільки радіосередовище є відкритим за своєю природою. Будь-який пристрій у зоні дії сигналу потенційно здатний перехоплювати трафік або здійснювати спроби несанкціонованого доступу до ресурсів мережі [3].

Під протоколом безпеки Wi-Fi слід розуміти не окремий механізм, а комплекс технічних правил і процедур. Він охоплює автентифікацію учасників з’єднання, шифрування даних, управління ключами та контроль цілісності інформації. Основне призначення такого протоколу полягає у забезпеченні конфіденційності, цілісності та доступності даних, що передаються у бездротовому середовищі [6].

Конфіденційність означає, що інформація доступна лише тим суб'єктам, яким вона призначена. У контексті Wi-Fi це досягається шифруванням переданих даних таким чином, що перехоплений трафік не може бути прочитаний без знання ключа шифрування. Цілісність гарантує, що дані не були змінені в процесі передачі - ні навмисно зловмисником, ні випадково через перешкоди в ефірі. Доступність забезпечує можливість легітимних користувачів отримувати доступ до мережевих ресурсів у будь-який момент, коли вони цього потребують, без затримок, спричинених атаками або некоректними налаштуваннями [6].

Основою будь-якого протоколу безпеки Wi-Fi є криптографічний захист. Криптографія вивчає методи перетворення інформації таким чином, щоб унеможливити її прочитання або модифікацію неуповноваженими особами. Стосовно бездротових мереж, криптографічний захист реалізується передусім через два підходи: симетричне та асиметричне шифрування [4].

При симетричному шифруванні один і той самий ключ використовується як для шифрування, так і для розшифрування. Основною перевагою такого підходу є висока швидкість обробки даних, що має важливе значення для мереж, у яких інформація передається у реальному часі. Серед алгоритмів цього класу, що застосовуються у протоколах Wi-Fi, слід виділити TKIP та AES. Алгоритм AES є блочним шифром із довжиною ключа 128, 192 або 256 біт. Він був стандартизований NIST у 2001 році та широко застосовується у системах захисту інформації, зокрема для шифрування носіїв даних, захисту мережевого трафіку та банківських операцій [5].

Асиметричне шифрування будується на парі ключів - відкритого та закритого. Відкритий ключ може бути загальнодоступним і призначений для шифрування, тоді як закритий зберігається у власника і слугує для розшифрування. Математична складність задачі відновлення закритого ключа за відкритим є гарантією безпеки такої системи. Такі алгоритми, як RSA та Diffie-Hellman, активно застосовуються при встановленні захищених з'єднань та обміні сесійними ключами [4]. Зокрема, протокол Diffie-Hellman покладено в основу механізму SAE у WPA3 - це дозволяє двом сторонам виробити спільний секрет через незахищений канал без його безпосередньої передачі.

Окремо слід сказати про хеш-функції. Вони перетворюють вхідні дані довільного розміру на рядок фіксованої довжини - хеш. Властивість однобічності означає, що відновити вхідні дані за хешем практично неможливо. Будь-яка зміна вихідних даних неминуче і непередбачувано змінює хеш, що дозволяє легко виявити факт несанкціонованої модифікації повідомлення. У протоколах Wi-Fi найчастіше застосовуються SHA-1, SHA-256 та HMAC - хеш-функція з використанням секретного ключа, що

забезпечує одночасно перевірку цілісності та автентифікацію джерела повідомлення [8].

Важливим поняттям у криптографічному захисті Wi-Fi є вектор ініціалізації (IV). IV - це випадкове або псевдовипадкове значення, що використовується разом із ключем шифрування для забезпечення унікальності процесу шифрування кожного пакета або блоку даних. Навіть за однакового ключа різні значення IV дають різний результат шифрування, що ускладнює статистичний криптоаналіз. Якість генерації та використання IV є критичним фактором безпеки протоколу. Саме недоліки цієї схеми стали однією з головних причин вразливості WEP [3].

Таким чином, протокол безпеки Wi-Fi - це інтегроване рішення, що поєднує різні криптографічні інструменти для захисту бездротових комунікацій. Без чіткого розуміння цих засад неможливо об'єктивно оцінити ефективність конкретних протоколів, що й стане предметом аналізу в наступних підрозділах.

1.2 Засоби та стандарти захисту бездротових мереж Wi-Fi

Розвиток стандартів безпеки для Wi-Fi мереж пов’язаний із діяльністю двох організацій: Інституту інженерів з електротехніки та електроніки (IEEE), що розробляє технічні специфікації сімейства 802.11, та Wi-Fi Alliance, який займається сертифікацією обладнання і просуванням стандартів у промисловості. Стандарти IEEE 802.11 охоплюють фізичний рівень передавання даних, рівень управління доступом до середовища (MAC) та механізми безпеки. У роботі враховано IEEE Std 802.11-2024 як актуальну редакцію базового стандарту, а також попередні редакції, необхідні для аналізу еволюції WEP, WPA, WPA2 та WPA3 [15].

Перший протокол безпеки для Wi-Fi - WEP (Wired Equivalent Privacy) - з'явився ще у 1997 році разом зі стандартом IEEE 802.11. Назва відображала задум: забезпечити рівень конфіденційності, порівнянний із провідними

мережами. Реалізовувалось це через алгоритм RC4 із ключем 40 або 104 біти та 24-бітним вектором ініціалізації. Проте вже на початку 2000-х дослідники виявили принципові вади в схемі використання IV, що фактично зробило WEP непридатним для практичного застосування. У 2004 році IEEE офіційно визнав WEP застарілим, а у 2012 році повністю вилучив його зі стандарту 802.11 [3].

У 2003 році Wi-Fi Alliance випустив WPA (Wi-Fi Protected Access) як тимчасовий замінник WEP. Ключовим нововведенням став протокол TKIP (Temporal Key Integrity Protocol), який генерує окремий ключ шифрування для кожного пакета, що значно ускладнює криптоаналіз. TKIP також запровадив 48-бітний порядковий номер пакета замість 24-бітного IV у WEP, що усунуло проблему повторення IV. Для корпоративних середовищ WPA підтримує автентифікацію через IEEE 802.1X та RADIUS-сервери [3].

У 2004 році з'явився WPA2, заснований на стандарті IEEE 802.11i. Головне досягнення - обов'язкове впровадження AES у режимі CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), що кардинально підвищило криптографічну стійкість. У 2006 році Wi-Fi Alliance зобов'язав усіх виробників сертифікованих пристроїв підтримувати WPA2. Упродовж наступних п'ятнадцяти років WPA2 залишався де-факто стандартом захисту Wi-Fi мереж у всьому світі [5].

У 2018 році Wi-Fi Alliance анонсував WPA3 - четверте покоління протоколів безпеки Wi-Fi. У персональному режимі WPA та WPA2 використовують PSK (Pre-Shared Key), тобто спільний попередньо встановлений пароль, на основі якого формується ключовий матеріал для захищеного з’єднання. У WPA3 замість підходу PSK застосовано протокол SAE (Simultaneous Authentication of Equals), який підвищує стійкість до атак перебору пароля. Для публічних мереж введено режим Enhanced Open із протоколом OWE (Opportunistic Wireless Encryption), що забезпечує шифрування трафіку навіть без використання пароля. У 2020 році підтримка WPA3 стала обов’язковою для нових пристроїв із сертифікацією Wi-Fi [7].

Окрім протокольних стандартів, важливу роль відіграють міжнародні нормативні документи у сфері інформаційної безпеки. Стандарт ISO/IEC 27001 визначає вимоги до системи управління інформаційною безпекою (СУІБ) і є основою для побудови комплексного захисту будь-якої організації. ISO/IEC 27002 містить практичні рекомендації щодо реалізації заходів безпеки, включаючи захист бездротових мереж. ISO/IEC 27005 присвячений управлінню ризиками інформаційної безпеки [9].

Рекомендації NIST (Національного інституту стандартів і технологій США) у сфері безпеки бездротових мереж викладені у спеціальній публікації NIST SP 800-153 «Guidelines for Securing Wireless Local Area Networks». Цей документ містить детальні рекомендації щодо вибору та налаштування протоколів безпеки Wi-Fi, управління ключами та моніторингу бездротової інфраструктури [9]. Для загальних вимог до паролів та інших автентифікаторів також враховано фінальну редакцію NIST SP 800-63B-4, оприлюднену у липні 2025 року, яка замінила попередню редакцію SP 800-63B [21].

В Україні нормативну базу у сфері інформаційної безпеки формують національні стандарти ДСТУ ISO/IEC 27001:2015 та ДСТУ ISO/IEC 27002:2015, що є адаптованими перекладами міжнародних аналогів. Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи захисту кіберпростору. Для об'єктів критичної інфраструктури діють додаткові вимоги, встановлені Кабінетом Міністрів України щодо захисту інформаційних систем [9].

Разом із протокольними засобами захист Wi-Fi мереж забезпечується й іншими інструментами. Фільтрація MAC-адрес має лише допоміжне значення, оскільки адресу легітимного пристрою можна перехопити та підмінити. Приховування SSID прибирає назву мережі з Beacon-кадрів, але не приховує сам факт її існування: SSID може бути відновлений з інших керувальних кадрів під час підключення клієнтів. VPN-тунелі забезпечують додаткове наскрізне шифрування, а WIDS/WIPS здійснюють моніторинг бездротового середовища та виявлення аномальної активності [3; 9].

1.3 Етапи встановлення захищеного з'єднання у Wi-Fi мережах

Підключення до захищеної Wi-Fi мережі - це не миттєва подія, а послідовний багатоетапний процес. Кожен його крок несе конкретну функцію: від виявлення мережі до формування унікальних ключів шифрування для конкретної сесії. Розуміння цього процесу є необхідним для оцінки того, де і яким чином можуть виникати вразливості [3].

На першому етапі клієнтський пристрій виявляє доступні мережі. Точка доступу постійно розсилає Beacon-кадри - широкомовні повідомлення з інтервалом зазвичай 100 мс, що містять SSID мережі, підтримувані швидкості та параметри безпеки. Клієнт може пасивно прослуховувати ефір або активно надсилати Probe Request-запити на всіх каналах, отримуючи у відповідь Probe Response від наявних точок доступу. Активне сканування є швидшим, але розкриває факт пошуку мережі.

Другий етап - формальна автентифікація на рівні 802.11. У переважній більшості сучасних мереж застосовується так звана відкрита автентифікація (Open System Authentication), яка насправді не перевіряє жодних облікових даних - це лише технічна процедура, що передує асоціації. Клієнт надсилає Authentication Request, точка доступу відповідає Authentication Response із кодом успіху. Реальна перевірка особи відбувається пізніше.

Третій етап - асоціація. Клієнт надсилає точці доступу Association Request із переліком підтримуваних можливостей, у тому числі алгоритмів шифрування та швидкостей передачі. Точка доступу відповідає Association Response, підтверджуючи або відхиляючи запит на підключення та призначаючи клієнту унікальний ідентифікатор асоціації (AID). З цього моменту клієнт вважається асоційованим із точкою доступу, але захищений канал ще не встановлено.

Четвертий етап залежить від типу мережі. У WPA2-Personal клієнт і точка доступу використовують спільний секрет PSK, після чого процедура 4-Way Handshake підтверджує наявність однакового ключового матеріалу та

формує сесійні ключі. У WPA3-Personal перед 4-Way Handshake виконується взаємна автентифікація SAE, у результаті якої формується PMK. У корпоративних мережах WPA2/WPA3-Enterprise використовується IEEE 802.1X: до успішної EAP-автентифікації точка доступу пропускає лише службовий автентифікаційний трафік, а після підтвердження облікових даних відкриває доступ до мережевих ресурсів [6; 7].

П'ятий, завершальний, етап - процедура 4-Way Handshake (чотириетапне рукостискання). Саме тут формуються реальні ключі шифрування для конкретної сесії. Перше повідомлення: точка доступу надсилає клієнту випадкове значення ANonce. Друге повідомлення: клієнт генерує своє випадкове значення SNonce, обчислює PTK на основі PMK, ANonce, SNonce та MAC-адрес обох сторін, надсилає SNonce і код цілісності MIC. Третє повідомлення: точка доступу верифікує MIC, підтверджуючи знання клієнтом правильного ключа, і надсилає GTK (груповий ключ). Четверте повідомлення: клієнт підтверджує отримання GTK. Після завершення рукостискання захищений канал встановлено [5].

Варто окремо зупинитися на ризиках, пов’язаних із 4-Way Handshake у WPA2-Personal. Оскільки PMK формується зі спільного пароля мережі, перехоплений обмін може використовуватися для багаторазової офлайн-перевірки варіантів пароля без подальшої взаємодії з точкою доступу. WPA3-Personal застосовує SAE, тому один пасивно перехоплений обмін не дає змоги необмежено перевіряти словникові варіанти офлайн. Водночас стійкість залежить від складності пароля, коректності реалізації SAE та відсутності небезпечного перехідного режиму [7; 14].

1.4 Процес автентифікації та авторизації користувачів

Автентифікацію та авторизацію часто плутають, хоча це принципово різні поняття. Автентифікація - це підтвердження того, що суб’єкт є тим, за кого себе видає. Авторизація - це вже рішення про те, до яких ресурсів і в

якому обсязі він має доступ. У контексті Wi-Fi мереж ці процеси реалізуються по-різному залежно від обраного режиму роботи [6].

У WPA2-Personal автентифікація ґрунтується на спільному секреті PSK, відомому клієнту і точці доступу. Пароль разом із SSID перетворюється на PMK за допомогою PBKDF2-HMAC-SHA1 із 4096 ітераціями. Це уповільнює перевірку варіантів, однак не компенсує використання слабкого пароля. У WPA3-Personal застосовується SAE - протокол взаємної автентифікації на основі пароля, який формує окремий ключовий матеріал для кожного сеансу та істотно підвищує стійкість до пасивних словникових атак [7; 14].

Для корпоративних мереж застосовується архітектура на основі IEEE 802.1X та протоколу EAP (Extensible Authentication Protocol). Логіка тут інша: до завершення автентифікації точка доступу блокує весь трафік клієнта, пропускаючи лише автентифікаційні повідомлення EAP. IEEE 802.1X визначає три ролі в цій архітектурі: суплікант (клієнт, що намагається підключитись), автентифікатор (точка доступу, що контролює доступ) та сервер автентифікації (RADIUS-сервер, що приймає остаточне рішення) [6].

EAP є розширюваним протоколом і підтримує безліч методів перевірки особи. EAP-TLS (Transport Layer Security) - найбільш захищений метод, що вимагає наявності сертифікатів X.509 як на клієнті, так і на сервері. Це забезпечує взаємну автентифікацію: клієнт перевіряє сервер, сервер - клієнта. EAP-PEAP (Protected EAP) захищає внутрішній метод автентифікації TLS-тунелем, при цьому клієнтський сертифікат не є обов'язковим - достатньо логіна і пароля всередині тунелю. EAP-TTLS аналогічний PEAP, але підтримує ширший набір внутрішніх методів, включаючи застарілі PAP та CHAP. EAP-FAST від Cisco розроблений для середовищ, де розгортання PKI є складним [6].

Сервер RADIUS (Remote Authentication Dial-In User Service) виконує функції AAA (автентифікація, авторизація, облік) у корпоративних Wi-Fi мережах. Протокол RADIUS визначений у RFC 2865 і широко підтримується всіма корпоративними рішеннями. Точка доступу в цій схемі є лише

посередником: вона передає облікові дані клієнта на RADIUS-сервер у вигляді Access-Request і отримує у відповідь або Access-Accept (доступ дозволено), або Access-Reject (доступ заборонено), або Access-Challenge (потрібна додаткова інформація). Крім самого рішення, сервер може передавати додаткові атрибути авторизації [6].

Динамічне призначення VLAN є одним із найважливіших інструментів авторизації у корпоративних Wi-Fi мережах. Залежно від ролі користувача (співробітник, гість, адміністратор) RADIUS-сервер передає точці доступу атрибут Tunnel-Private-Group-ID із номером відповідного VLAN. Таким чином, навіть підключаючись до однієї точки доступу, різні категорії користувачів опиняються в ізольованих мережевих сегментах із різними правами доступу. Це суттєво обмежує можливі наслідки компрометації будь-якого пристрою [6].

1.5 Аналіз шифрування та передавання даних у Wi-Fi мережах

Еволюція алгоритмів шифрування у Wi-Fi протоколах відображає загальну картину розвитку криптографії: кожне нове покоління виправляло помилки попередника і підвищувало планку захисту. Розглянемо, як змінювались підходи до шифрування від WEP до WPA3 [3].

WEP використовував потоковий шифр RC4 із ключем 40 або 104 біти. RC4 генерує псевдовипадковий потік бітів (keystream), що накладається на відкритий текст операцією XOR. Проблема WEP полягала не в самому RC4, а в схемі формування ключа для кожного пакета: ключ складався з постійного WEP-ключа та 24-бітного IV, що передавався у відкритому вигляді. При достатньому обсязі перехопленого трафіку IV починали повторюватись (за принципом «дня народження» - при 24-бітному IV повторення очікується приблизно після 5000 пакетів при певних умовах), що відкривало можливість для статистичного відновлення ключа. Дослідники Флурер, Мантін та Шамір ще у 2001 році описали практичну атаку на RC4/WEP [3].

TKIP у WPA зберіг RC4 як базовий алгоритм, але кардинально змінив схему управління ключами. Для кожного пакета генерується унікальний ключ шифрування - так звана «суміш ключів» (key mixing) - на основі тимчасового ключа TK, MAC-адреси відправника та 48-бітного порядкового номера пакета. Замість простого конкатенування ключа і IV, як у WEP, TKIP виконує складне перемішування, що усуває вразливості слабких ключів RC4. Також введено 64-бітний код цілісності MIC (алгоритм Michael), що захищає від підробки пакетів. Проте і TKIP виявився вразливим: атака Бека-Тевса 2008 року продемонструвала можливість часткового розшифрування за певних умов [3].

Впровадження WPA2 ознаменувало перехід на принципово інший алгоритм - AES у режимі CCMP. AES є блочним шифром з розміром блоку 128 біт та ключем 128, 192 або 256 біт. На відміну від потокового RC4, блочний шифр обробляє дані фіксованими блоками, що дає змогу застосовувати різні режими роботи з різними властивостями безпеки. Режим CCM поєднує в одній операції шифрування (CTR - режим лічильника) та обчислення коду автентифікації (CBC-MAC), забезпечуючи одночасно конфіденційність і цілісність із 128-бітним ключем. AES є міжнародним стандартом, стандартизованим NIST у 2001 році, і не має відомих практичних атак на базовий алгоритм [5].

WPA3 розширив криптографічні можливості, додавши підтримку GCMP-256 - режиму AES на основі лічильника Галуа із 256-бітним ключем. Режим GCM поєднує режим CTR для шифрування з хешуванням Галуа для обчислення коду автентифікації. Ключова перевага GCM перед CCM - можливість паралельної обробки блоків, що забезпечує вищу продуктивність на сучасному апаратному забезпеченні. У режимі WPA3-Enterprise 192-bit mode також застосовується HMAC-SHA-384, що відповідає вимогам Suite B криптографії, рекомендованої АНБ США для захисту матеріалів із грифом «Секретно» [7].

Фізично дані передаються у вигляді кадрів стандарту IEEE 802.11 чіткої структури. Кожен кадр містить заголовок MAC з адресами відправника і

отримувача, порядковим номером та іншою службовою інформацією; корисне навантаження із зашифрованими даними; поле перевірки кадру FCS (Frame Check Sequence) для виявлення помилок передачі. При використанні CCMP структура кадру розширюється: додається 8-байтовий заголовок CCMP (що містить порядковий номер пакета для захисту від replay-атак) та 8-байтовий код цілісності MIC у кінці кадру. Таким чином, накладні витрати CCMP складають 16 байт на кадр [5].

1.6 Збереження та управління ключами безпеки

Надійність алгоритму шифрування не гарантує захищеності мережі у разі неналежного управління ключами. Тому управління ключами є одним із ключових елементів системи безпеки Wi-Fi. У стандартах WPA2 та WPA3 криптографічні ключі, службові параметри і похідні значення, які використовуються для встановлення захищеного з'єднання, організовані у вигляді ієрархії. Кожен рівень цієї ієрархії виконує окрему функцію: формування головного ключа, генерацію сесійних ключів, шифрування трафіку та захист групових повідомлень [5].

На вершині ієрархії знаходиться PMK (Pairwise Master Key) - головний ключ, що є відправною точкою для всього подальшого ключового матеріалу. У персональному режимі PMK формується з пароля мережі та її SSID за допомогою функції PBKDF2-HMAC-SHA1 із 4096 ітераціями. Включення SSID у процес формування PMK є важливим заходом безпеки: воно унеможливлює використання попередньо обчислених таблиць (rainbow tables) для різних мереж - таблиця, обчислена для мережі «HomeNet», не підходить для «OfficeNet», навіть якщо пароль однаковий. В корпоративному режимі PMK передається безпосередньо з RADIUS-сервера після успішної EAP-автентифікації і є унікальним для кожної сесії [6].

З PMK у процесі 4-Way Handshake похідним чином формується PTK (Pairwise Transient Key). Для цього використовуються PMK, два випадкових

числа - ANonce від точки доступу і SNonce від клієнта - та MAC-адреси обох сторін. Включення випадкових чисел гарантує, що PTK буде унікальним для кожної сесії, навіть якщо PMK залишається незмінним. PTK має довжину 512 біт і складається з трьох функціональних компонентів: KCK (Key Confirmation Key, 128 біт) - для перевірки цілісності повідомлень під час рукостискання; KEK (Key Encryption Key, 128 біт) - для шифрування GTK при передачі; TK (Temporal Key, 128 або 256 біт) - безпосередньо для шифрування даних сесії [5].

GTK (Group Temporal Key) призначений для шифрування широкомовного та багатоадресного трафіку. На відміну від PTK, GTK є спільним для всіх клієнтів мережі - він генерується точкою доступу і передається кожному клієнту в зашифрованому вигляді за допомогою KEK. Для підтримки актуального рівня захисту GTK регулярно оновлюється - зокрема, при відключенні будь-якого клієнта від мережі, щоб він не міг розшифровувати трафік інших клієнтів після завершення сесії [5].

Що стосується зберігання ключів на пристроях: у Windows для цього використовується Credential Manager із механізмом DPAPI (Data Protection API), що прив'язує захист до облікового запису користувача або комп'ютера. Ключі шифруються за допомогою похідного від пароля облікового запису матеріалу, що унеможливлює їх читання іншими користувачами або процесами без відповідних прав. У Linux-системах ключі зберігаються у конфігураційних файлах NetworkManager або wpa_supplicant із обмеженими правами доступу на рівні файлової системи [4].

Принциповим нововведенням WPA3 є підтримка Forward Secrecy (прямої секретності), що реалізується через протокол SAE. Пряма секретність означає, що кожна сесія використовує унікальний набір ключів, який не може бути відновлений лише на основі довгострокового секрету, зокрема пароля мережі. Якщо зловмисник отримає пароль після завершення сеансу зв’язку, це не дасть йому змоги розшифрувати раніше записаний трафік. Ця властивість

відрізняє WPA3 від WPA2, де компрометація пароля може створити ризик для раніше перехоплених даних [7].

1.7 Загрози безпеці Wi-Fi мереж та методи їх нейтралізації

Відкрита природа радіосередовища обумовлює широкий спектр загроз для Wi-Fi мереж. Усвідомлення того, які атаки реально можливі і чому, є передумовою для вибору адекватних засобів захисту [3].

Пасивне прослуховування (eavesdropping) - одна з найпростіших атак. Зловмисник переводить бездротовий адаптер у режим монітора і записує всі пакети у зоні прийому сигналу, не втручаючись у роботу мережі. Пасивне прослуховування практично неможливо виявити, оскільки зловмисник не генерує жодного трафіку. Захист - надійне шифрування: WPA2/WPA3 робить перехоплені дані практично марними без знання ключів [3].

Атака «людина посередині» (Man-in-the-Middle, MitM) передбачає, що зловмисник розміщується між клієнтом і точкою доступу, перехоплюючи та потенційно модифікуючи трафік. Окремий різновид - Evil Twin (підробна точка доступу): зловмисник розгортає точку доступу з ідентичним SSID і більшою потужністю сигналу, змушуючи клієнтів підключатись до неї замість легітимної. Після підключення весь трафік клієнта проходить через контрольований зловмисником пристрій. Протидія включає взаємну автентифікацію (WPA3-Enterprise з EAP-TLS), використання HTTPS та VPN [3].

Атака KRACK (Key Reinstallation Attack), виявлена дослідником Матті Ванхофом у 2017 році, експлуатувала вразливість у реалізації 4-Way Handshake в WPA2. Зловмисник примушував клієнта повторно використовувати вже задіяний ключ шифрування, що призводило до повторного використання потокового шифру і відкривало можливість для розшифрування трафіку або підробки пакетів. Вразливість була закрита

оновленнями прошивок для більшості пристроїв; WPA3 є стійким до неї завдяки SAE [5].

Атака PMKID, описана дослідником Йенсом Штойбе у 2018 році, дозволяє отримати матеріал для офлайн-перебору пароля безпосередньо від точки доступу - без потреби чекати на підключення будь-якого клієнта. PMKID обчислюється як HMAC-SHA1 від рядка «PMK Name», PMK, MAC-адреси точки доступу та MAC-адреси клієнта. Оскільки PMKID міститься у першому повідомленні 4-Way Handshake, яке точка доступу надсилає у відповідь на будь-який запит підключення, зловмисник може отримати його пасивно. Захист: перехід на WPA3 або використання складного пароля [5].

Одним із різновидів DoS-атак у Wi-Fi мережах є надсилання підроблених deauthentication- або disassociation-фреймів, що спричиняє відключення клієнтів. У ранніх реалізаціях такі керувальні фрейми не мали криптографічного захисту. Обов’язкове застосування Protected Management Frames у WPA3 суттєво знижує можливість їх підроблення після встановлення захищеного з’єднання, однак не усуває всі способи радіоперешкод і відмови в обслуговуванні [7].

Атака методом перебору паролів (Brute Force / Dictionary Attack) спрямована на відновлення PSK-пароля після захоплення 4-Way Handshake. Зловмисник перебирає варіанти паролів і для кожного обчислює PMK та відповідні ключі, порівнюючи обчислений MIC із перехопленим. Ефективність атаки залежить від складності пароля та обчислювальних ресурсів зловмисника. Використання GPU суттєво прискорює перебір - сучасні відеокарти здатні перевіряти мільярди варіантів за секунду [3].

Wardriving - методика виявлення бездротових мереж шляхом переміщення місцевістю з відповідним обладнанням (ноутбук або смартфон із спеціалізованим ПЗ та GPS-приймачем). Зібрані дані можуть використовуватись для подальшого злому або картографування мереж. Відомі онлайн-бази даних (WiGLE.net) містять мільярди записів про Wi-Fi мережі по

всьому світу. Для зниження ризику рекомендується обмежувати потужність сигналу точки доступу та контролювати список підключених пристроїв [3].

Висновки до першого розділу.

У першому розділі систематизовано теоретичні засади захисту бездротових мереж Wi-Fi. Встановлено, що протокол безпеки Wi-Fi є багаторівневим технічним рішенням, яке поєднує механізми автентифікації, шифрування та управління ключами. Розглянуто еволюцію стандартів захисту від WEP до WPA3, а також нормативну базу у сфері безпеки бездротових мереж, зокрема стандарти ISO/IEC та рекомендації NIST. Визначено актуальні загрози безпеці Wi-Fi мереж і методи протидії їм, що створює теоретичну основу для подальшого аналізу сучасних протоколів захисту.

РОЗДІЛ 2
АНАЛІЗ МОЖЛИВОСТЕЙ СУЧАСНИХ ПРОТОКОЛІВ WI-FI ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

2.1 Методи автентифікації у протоколах WEP, WPA, WPA2, WPA3

Автентифікація визначає, хто саме отримає доступ до мережі, а тому її надійність є першочерговою умовою безпеки. Аналізуючи еволюцію методів автентифікації у стандартах Wi-Fi, можна чітко простежити, як кожне покоління протоколів намагалось усунути вразливості попередника [3].

WEP підтримував два підходи до автентифікації: відкриту системну автентифікацію (Open System Authentication) та автентифікацію зі спільним ключем (Shared Key Authentication). При відкритій автентифікації точка доступу приймає будь-який запит на підключення без перевірки - фактично це означало повну відсутність контролю доступу на рівні автентифікації. Шифрування у такому випадку мало забезпечувати конфіденційність, але не контроль доступу.

Автентифікація зі спільним ключем у WEP використовувала механізм виклику-відповіді (challenge-response): точка доступу надсилала клієнту відкритий текст обсягом 128 байт, клієнт шифрував його WEP-ключем і надсилав результат назад. Точка доступу порівнювала отримане значення з власним результатом шифрування того самого тексту. Такий підхід виявився менш безпечним, ніж відкрита автентифікація, оскільки зловмисник міг отримати пару «відкритий текст - шифротекст», що спрощувало криптоаналіз RC4 [3].

WPA запровадив два режими автентифікації, що збереглись у всіх наступних поколіннях протоколів. Персональний режим (WPA-Personal або WPA-PSK) використовує попередньо розповсюджений ключ (Pre-Shared Key, PSK) - пароль, відомий усім учасникам мережі. PSK перетворюється на PMK за допомогою функції PBKDF2 (Password-Based Key Derivation Function 2) із

4096 ітераціями хешування SHA-1. Велика кількість ітерацій навмисно сповільнює обчислення, що ускладнює атаки перебором - кожна спроба пароля вимагає значних обчислювальних ресурсів [3].

Корпоративний режим WPA (WPA-Enterprise) базується на стандарті IEEE 802.1X та інфраструктурі RADIUS-серверів, що забезпечує індивідуальну автентифікацію кожного користувача з використанням унікальних облікових даних. Це принципово відрізняє корпоративний режим від персонального: у разі компрометації облікових даних одного користувача не потрібно змінювати пароль для всієї мережі - достатньо заблокувати конкретний обліковий запис [6].

WPA2 зберіг архітектуру PSK та 802.1X, але вдосконалив криптографічну складову. В корпоративному режимі опціональним, а згодом обов'язковим, став захист управляючих фреймів (Management Frame Protection, MFP) відповідно до IEEE 802.11w. Суттєвою вадою залишилась вразливість персонального режиму до офлайн-атак: зловмисник, перехопивши 4-Way Handshake, може підбирати пароль без будь-якої взаємодії з точкою доступу - необмежену кількість спроб з необмеженою швидкістю [5].

WPA3 вирішив проблему офлайн-атак кардинально: замість PSK тут використовується протокол SAE (Simultaneous Authentication of Equals). SAE базується на криптографічному протоколі Dragonfly Key Exchange - різновиді обміну ключами на основі еліптичних кривих. Ключовою особливістю SAE є те, що обидві сторони одночасно доводять знання пароля без його безпосередньої передачі. Для перевірки кожного варіанту пароля зловмисник змушений взаємодіяти з точкою доступу - масовий офлайн-перебір стає неможливим. Крім того, кожна успішна SAE-автентифікація породжує унікальний PMK, що забезпечує Forward Secrecy [7].

У WPA3 також покращено захист для корпоративних мереж. WPA3-Enterprise у режимі 192-bit забезпечує мінімальний рівень криптографічної стійкості 192 біти, що відповідає вимогам Suite B криптографії. Обов'язковим є використання EAP-методів із взаємною автентифікацією, зокрема EAP-TLS

із сертифікатами на основі алгоритмів P-384 або вище. Це забезпечує рівень захисту, придатний для організацій із найвищими вимогами до безпеки, зокрема державних установ та об'єктів критичної інфраструктури [7].

Порівняльна характеристика методів автентифікації наведена у таблиці 2.1.

Таблиця 2.1 - Порівняльна характеристика методів автентифікації Wi-Fi протоколів

Характеристика	**WEP**	**WPA**	**WPA2**	**WPA3**
Метод автентифікації	Open / Shared Key	PSK / 802.1X	PSK / 802.1X	SAE / 802.1X
Алгоритм обміну ключами	Статичний ключ	4-Way Handshake	4-Way Handshake	Dragonfly (SAE)
Взаємна автентифікація	Ні	Часткова	Часткова	Повна
Захист від перебору	Відсутній	Слабкий	Слабкий	Сильний
Forward Secrecy	Ні	Ні	Ні	Так
Підтримка EAP	Ні	Так	Так	Так

Як видно з таблиці 2.1, між поколіннями протоколів існують принципові відмінності у підходах до автентифікації. Якщо WEP фактично не забезпечував надійної перевірки особи, то WPA3 реалізує повноцінну взаємну автентифікацію з ефективним захистом від атак перебору та прямою секретністю, що відповідає найсучаснішим вимогам до захисту бездротових мереж.

2.2 Методи шифрування інформації у бездротових мережах

Шифрування - це той механізм, що безпосередньо захищає дані від перехоплення. Розглянемо детально, які алгоритми використовувались у кожному поколінні протоколів Wi-Fi і чому відбувалась їхня зміна [3].

WEP покладався на потоковий шифр RC4 із ключем 40 або 104 біти. RC4 генерує псевдовипадковий потік бітів (keystream), що накладається на відкритий текст операцією XOR. Алгоритм є відносно простим у реалізації і

забезпечує високу швидкість шифрування, що зробило його привабливим для застосування у мережевих пристроях початку 2000-х з обмеженими обчислювальними ресурсами. Проте критична вада WEP полягала не у самому RC4, а у схемі формування ключа шифрування для кожного пакета [3].

24-бітний вектор ініціалізації передавався у відкритому вигляді разом із зашифрованим пакетом. При достатньому обсязі перехопленого трафіку IV починали повторюватись, що відкривало можливість для статистичного аналізу. Дослідники Флурер, Мантін та Шамір у 2001 році описали клас слабких ключів RC4, що утворюються при певних значеннях IV, і показали, що аналіз лише пакетів зі слабкими IV дозволяє відновити ключ шифрування. Це стало теоретичним підґрунтям для практичних інструментів злому, таких як Aircrack-ng та AirSnort [3].

TKIP у складі WPA зберіг RC4 як базовий алгоритм, але повністю переробив схему управління ключами. Основою TKIP є механізм «суміші ключів» (key mixing): для кожного пакета генерується унікальний 128-бітний ключ RC4, що є функцією тимчасового ключа TK, MAC-адреси відправника та 48-бітного порядкового номера пакета (TSC - TKIP Sequence Counter). Використання 48-бітного лічильника замість 24-бітного IV унеможливлює їх повторення протягом реалістичного терміну використання мережі [3].

Додатково TKIP запровадив алгоритм Michael - 64-бітний код цілісності повідомлення (MIC), що обчислюється для кожного пакета на основі його вмісту та ключа цілісності. Це захищає від підробки пакетів. Крім того, TKIP містить механізм контрмір: при виявленні двох невалідних MIC протягом однієї хвилини точка доступу блокує підключення клієнта на 60 секунд. Незважаючи на ці покращення, атака Бека-Тевса 2008-2009 років показала, що за певних умов можна розшифрувати окремі пакети, підробляючи MIC-коди [3].

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), що став обов'язковим у WPA2, є принципово іншим рішенням. В основі CCMP лежить блочний шифр AES (Advanced Encryption Standard) у

режимі CCM. AES обробляє дані блоками по 128 біт з ключем 128, 192 або 256 біт. На відміну від потокового RC4, блочний шифр не має відомого класу слабких ключів і вважається значно більш надійним [5].

Режим CCM поєднує два операційні режими AES: CTR (Counter Mode) для шифрування даних та CBC-MAC (Cipher Block Chaining - Message Authentication Code) для обчислення коду автентифікації. CTR перетворює блочний шифр на потоковий, шифруючи послідовно зростаючі значення лічильника та накладаючи результат на відкритий текст. CBC-MAC обчислює код автентифікації шляхом послідовного шифрування блоків із результатом попереднього операції. Поєднання обох режимів в одному проході даних забезпечує одночасно конфіденційність і цілісність [5].

У WPA2 CCMP використовує 128-бітний ключ AES та 48-бітний порядковий номер пакета (PN - Packet Number), що передається у відкритому 8-байтовому заголовку CCMP. PN відіграє роль вектора ініціалізації і гарантує унікальність шифрування для кожного пакета. Код автентифікації MIC має довжину 64 біти і захищає не лише корисне навантаження, а й частину заголовка MAC-рівня. AES-CCMP вважається криптографічно стійким і на сьогодні не має відомих практичних атак на базовий алгоритм [5].

GCMP (Galois/Counter Mode Protocol), запроваджений у WPA3, використовує режим GCM (Galois/Counter Mode) алгоритму AES. GCM поєднує режим CTR для шифрування з хешуванням Галуа (GHASH) для обчислення коду автентифікації. На відміну від CBC-MAC у CCMP, хешування Галуа допускає паралельну обробку, що суттєво підвищує продуктивність на сучасному апаратному забезпеченні з підтримкою векторних інструкцій [7].

У базовому режимі WPA3-Personal використовується GCMP-128 із 128-бітним ключем. У режимі WPA3-Enterprise 192-bit застосовується GCMP-256 із 256-бітним ключем та HMAC-SHA-384 для забезпечення цілісності управляючих фреймів. Код автентифікації MIC у GCMP має довжину 128 біт

(порівняно з 64 бітами у CCMP), що підвищує стійкість до підробки пакетів [7].

Таблиця 2.2 - Порівняльний аналіз методів шифрування у протоколах Wi-Fi

Параметр	**WEP**	**WPA/TKIP**	**WPA2/CCMP**	**WPA3/GCMP**
Базовий алгоритм	RC4	RC4	AES	AES
Режим роботи	Потоковий	TKIP	CCM	GCM
Довжина ключа (біт)	40 / 104	128	128	128 / 256
Розмір IV/PN (біт)	24	48	48	48
Захист цілісності	CRC-32	Michael MIC	CBC-MAC	GHASH
Довжина MIC (біт)	32	64	64	128
Паралельна обробка	Ні	Ні	Частково	Так
Рівень безпеки	Критично низький	Середній	Високий	Дуже високий

Дані таблиці 2.2 демонструють послідовне підвищення рівня захисту від WEP до WPA3. Розвиток протоколів відбувався від використання слабкого потокового шифру зі статичними ключами до застосування стійких алгоритмів шифрування, динамічного формування ключів, механізмів контролю цілісності та підтримки апаратного прискорення.

2.3 Захист переданих даних та управління доступом у Wi-Fi мережах

Криптографічні механізми шифрування та автентифікації - це лише частина системи захисту Wi-Fi мереж. Не менш важливими є засоби забезпечення цілісності даних, захист управляючих фреймів та інструменти управління доступом до мережевих ресурсів [5].

Цілісність даних у різних протоколах забезпечується по-різному. WEP використовував CRC-32 - циклічний надлишковий код довжиною 32 біти. CRC-32 розроблявся для виявлення випадкових помилок передачі, а не для захисту від навмисної модифікації. Оскільки CRC-32 є лінійною функцією, зловмисник може обчислити необхідну зміну контрольної суми при

модифікації зашифрованого тексту без знання ключа, що робить захист цілісності у WEP практично неефективним [3].

TKIP використовує алгоритм Michael із 64-бітним кодом MIC. Michael враховує вміст пакета та секретний ключ цілісності, однак має обмежені криптографічні властивості. За результатами досліджень, підробка MIC може бути здійснена приблизно за 2 у 29-му степені операцій, що є недостатнім рівнем стійкості для сучасних вимог безпеки. Саме тому у TKIP було запроваджено механізм контрзаходів у разі виявлення підробки [3].

CCMP у WPA2 застосовує CBC-MAC із 64-бітним тегом автентифікації. CBC-MAC є значно більш стійким, ніж Michael, і захищає як корисне навантаження, так і частину заголовка MAC-рівня (MPDU Header). Це захищає від підробки адрес відправника та отримувача у зашифрованому пакеті [5].

GCMP у WPA3 формує 128-бітний тег автентифікації на основі хешування Галуа, що є найбільш стійким із розглянутих варіантів. Збільшення довжини тега вдвічі порівняно з CCMP суттєво підвищує стійкість до атак методом підбору коду автентифікації [7].

Окремою проблемою є захист управляючих фреймів (Management Frame Protection, MFP). Управляючі фрейми стандарту 802.11, зокрема Beacon, Probe Response, Association Request/Response, Disassociation та Deauthentication, у ранніх версіях протоколів не захищались від підробки. Унаслідок цього зловмисник міг сформувати підроблений фрейм деавтентифікації від імені точки доступу та примусово відключати клієнтів від мережі. Така вразливість використовується в атаках на доступність та як підготовчий етап для атак типу Evil Twin [3].

Стандарт IEEE 802.11w, прийнятий у 2009 році та інтегрований у WPA2 як опція, а у WPA3 вже обов'язковий, вирішує цю проблему через цифровий підпис управляючих фреймів. Захищені управляючі фрейми (Deauthentication, Disassociation та інші) шифруються та автентифікуються за допомогою ключів, встановлених у процесі 4-Way Handshake. Таким чином, підробити захищений фрейм без знання ключа стає практично неможливим [7].

Управління доступом у Wi-Fi мережах реалізується на кількох рівнях. Найпростіший - фільтрація MAC-адрес: точка доступу перевіряє MAC-адресу кожного пристрою, що намагається підключитись, і порівнює з дозволеним списком. Незважаючи на простоту реалізації, фільтрація MAC-адрес не є ефективним засобом захисту в сучасних умовах: MAC-адреса передається у відкритому вигляді в кожному пакеті, тому зловмисник може легко дізнатись дозволену адресу і підробити її [3].

Значно ефективнішим є контроль доступу на основі IEEE 802.1X. До завершення автентифікації логічний порт клієнта на точці доступу залишається заблокованим, і через нього проходять лише EAP-пакети, необхідні для перевірки облікових даних. Після успішної автентифікації RADIUS-сервер може передавати точці доступу додаткові атрибути авторизації. Атрибут Tunnel-Private-Group-ID визначає номер VLAN, до якого буде віднесено клієнта. Атрибут Session-Timeout встановлює максимальну тривалість сесії, а Idle-Timeout визначає час бездіяльності, після якого з’єднання розривається [6].

Сегментація мережі через VLAN є потужним інструментом управління доступом. Динамічне призначення VLAN дозволяє розміщувати різні категорії користувачів - співробітників, гостей, IoT-пристрої, підрядників - у ізольованих мережевих сегментах із відповідними політиками безпеки. Це суттєво обмежує можливі наслідки компрометації окремого пристрою: зловмисник, який отримав контроль над IoT-пристроєм у відповідному VLAN, не має доступу до корпоративних серверів в іншому сегменті [6].

WPA3 запровадив режим Enhanced Open (OWE - Opportunistic Wireless Encryption) для публічних мереж. OWE забезпечує шифрування трафіку між клієнтом і точкою доступу навіть за відсутності пароля, використовуючи обмін ключами Діффі-Хеллмана. Кожна сесія використовує унікальну пару ключів, що унеможливлює розшифрування трафіку інших клієнтів тієї самої мережі - навіть якщо вони підключені до тієї самої точки доступу. Хоча OWE

не захищає від активних MitM-атак, він суттєво підвищує конфіденційність у публічних місцях порівняно з повністю відкритими мережами [7].

Системи WIDS (Wireless Intrusion Detection System) та WIPS (Wireless Intrusion Prevention System) доповнюють криптографічні засоби захисту. WIDS здійснює пасивний моніторинг бездротового середовища, виявляючи ознаки атак: несанкціоновані точки доступу (rogue AP), аномальні управляючі фрейми, спроби деавтентифікації клієнтів, сканування мережі, підозрілу активність конкретних пристроїв. WIPS іде далі і здатна активно нейтралізувати виявлені загрози, зокрема через примусове відключення клієнтів несанкціонованих точок доступу [3].

Важливим аспектом захисту Wi-Fi мереж є безпека на рівні застосунків. Навіть при використанні WPA3 доцільно застосовувати захищені протоколи прикладного рівня: HTTPS замість HTTP, SFTP замість FTP, SSH замість Telnet. Це забезпечує наскрізне шифрування (end-to-end encryption), за якого дані залишаються зашифрованими протягом усього шляху від відправника до отримувача, а не лише на ділянці бездротового з’єднання. Такий підхід зменшує ризики навіть у разі часткової компрометації Wi-Fi мережі [9].

Використання VPN (Virtual Private Network) є ще одним ефективним засобом додаткового захисту. VPN створює зашифрований тунель між клієнтом і VPN-сервером, через який проходить весь трафік клієнта. Навіть якщо зловмисник розгорнув підробну точку доступу і перехоплює трафік, зашифрований VPN-тунель унеможливлює читання або модифікацію даних. Корпоративні рішення, як правило, використовують IPSec або SSL/TLS-базовані VPN, тоді як для персонального використання популярними є WireGuard та OpenVPN [9].

Висновки до другого розділу.

У другому розділі проведено аналіз можливостей сучасних протоколів Wi-Fi щодо захисту бездротових мереж. Досліджено еволюцію методів автентифікації - від слабких механізмів WEP до взаємної автентифікації та

прямої секретності у WPA3. Проаналізовано алгоритми шифрування: RC4/WEP, TKIP, AES-CCMP у WPA2 та GCMP у WPA3. Розглянуто механізми захисту переданих даних, зокрема MFP, IEEE 802.1X, динамічне призначення VLAN, WIDS/WIPS та OWE. Встановлено, що ефективний захист Wi-Fi мережі потребує поєднання сучасного протоколу, правильного налаштування та додаткових засобів контролю доступу.

РОЗДІЛ 3
ОЦІНЮВАННЯ ТА ПРАКТИЧНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПРОТОКОЛІВ WI-FI ДЛЯ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

3.1 Аналіз ефективності протоколів Wi-Fi у забезпеченні захисту бездротових мереж

Оцінювання ефективності протоколів безпеки Wi-Fi є комплексним завданням, що потребує систематизованого підходу. Ефективність протоколу захисту визначається не лише криптографічною стійкістю базових алгоритмів, а й сукупністю взаємопов'язаних чинників: надійністю механізмів автентифікації, ефективністю управління ключами, рівнем захисту від відомих атак, продуктивністю та практичною реалізованістю у реальних умовах [9].

Для системного оцінювання ефективності протоколів у цій роботі застосовується багатокритеріальний підхід, що передбачає виділення ключових критеріїв оцінювання, визначення їх відносної ваги відповідно до пріоритетів безпеки та обчислення інтегральної оцінки для кожного протоколу. Такий підхід дозволяє отримати об'єктивну порівняльну характеристику протоколів, враховуючи різноманітні аспекти їхнього функціонування і виключаючи суб'єктивність оцінок [9].

Ефективність протоколу WEP з позицій захисту інформації є критично низькою. Алгоритм RC4 із 24-бітним вектором ініціалізації має принципові вразливості: при перехопленні значної кількості пакетів зловмисник може відновити ключ шифрування з високою ймовірністю. Практичні інструменти, зокрема Aircrack-ng, автоматизують процес відновлення WEP-ключа за наявності достатнього обсягу трафіку. Механізм перевірки цілісності CRC-32 є лінійною функцією і не є криптографічним кодом автентифікації, тому не забезпечує належного захисту від навмисної модифікації пакетів. IEEE визнав WEP застарілим у 2004 році та вилучив його зі стандарту 802.11 у 2012 році [3].

Ефективність протоколу WPA суттєво вища порівняно з WEP: динамічна зміна ключів TKIP та криптографічний код цілісності Michael усувають основні вразливості попередника. Проте WPA зберігає ряд проблем. По-перше, RC4 як базовий алгоритм має теоретичні слабкості, що підтвердила атака Бека-Тевса у 2008-2009 роках - вона дозволяє розшифровувати окремі пакети за 12-15 хвилин за певних умов. По-друге, Michael із 64-бітним MIC є відносно слабким кодом цілісності. По-третє, WPA-Personal залишається вразливим до офлайн-атак методом перебору словника після захоплення 4-Way Handshake [3].

Ефективність WPA2 є значно вищою: AES-CCMP не має відомих практичних криптографічних атак на базовий алгоритм шифрування. Атака KRACK 2017 року була спрямована не на AES, а на реалізацію процедури 4-Way Handshake і усунена оновленнями програмного забезпечення переважної більшості пристроїв. Атака PMKID 2018 року дозволяє здійснювати офлайн-перебір пароля PSK, однак при використанні складних паролів (понад 15-20 символів) є практично нездійсненною з огляду на обчислювальні ресурси, що вимагаються. WPA2-Enterprise із взаємною автентифікацією EAP-TLS є виключно стійким рішенням при коректному розгортанні [5].

WPA3 є найсучаснішим із розглянутих стандартів захисту Wi-Fi мереж. SAE істотно обмежує можливості пасивного офлайн-перебору паролів і забезпечує пряму секретність для окремих сеансів. Обов’язкове застосування Protected Management Frames знижує ризик підроблення кадрів деавтентифікації та роз’єднання після встановлення захищеного з’єднання, але не усуває всі види DoS-атак і радіоперешкод. Дослідження Dragonblood 2019 року виявило ризики в окремих реалізаціях SAE та перехідних режимах, тому для WPA3 важливими залишаються актуальні прошивки й коректне налаштування обладнання [14].

3.2 Порівняльний аналіз протоколів WEP, WPA, WPA2, WPA3 за результатами теоретичного оцінювання та практичного тестування окремих типових конфігурацій

Порівняльний аналіз протоколів здійснюється за методологією багатокритеріального оцінювання із застосуванням шкали від 1 до 5 балів для кожного визначеного критерію безпеки. Шкала оцінювання має такий зміст: 1 - незадовільно, 2 - низький рівень, 3 - задовільно, 4 - добре, 5 - відмінно. У межах практичної частини безпосередньо перевірено типові конфігурації WEP та WPA2, оскільки саме ці режими були доступні в лабораторному середовищі та дають змогу показати дві ключові проблеми: принципову криптографічну вразливість застарілого WEP і залежність WPA2 від якості пароля та налаштувань. Протоколи WPA та WPA3 у цьому підрозділі оцінюються на основі теоретичного аналізу стандартів, рекомендацій NIST, матеріалів Wi-Fi Alliance та сучасних досліджень [7; 9; 14; 15].

Практичне тестування WPA та WPA3 у межах дослідження не виконувалося як окремий повний експеримент. WPA є проміжним і застарілим протоколом, який у сучасних мережах майже не застосовується окремо від WPA2, а його практична перевірка не дала б додаткової цінності порівняно з аналізом TKIP та PSK. Повноцінне тестування WPA3 потребує окремого обладнання з підтримкою SAE, WPA3-Personal, WPA3-Enterprise, обов’язкового MFP та відповідних засобів аналізу. Тому висновки щодо WPA та WPA3 сформульовано як результат теоретичного оцінювання, а не як результат прямого практичного зламу або повної експериментальної перевірки всіх режимів роботи.

Стійкість алгоритму шифрування (максимум 5 балів). Критерій враховує криптографічну міцність базового алгоритму, довжину ключа, якість генерації векторів ініціалізації та наявність відомих практичних атак. WEP - 1 бал: RC4 із 24-бітним IV є принципово зламним. WPA - 3 бали: TKIP покращив управління ключами, але зберіг RC4 із його теоретичними слабкостями. WPA2 - 4 бали: AES-CCMP є криптографічно стійким, але 64-бітний MIC є дещо консервативним.

WPA3 - 5 балів: GCMP-256 із 128-бітним MIC представляє сучасний рівень захисту [5].

Надійність автентифікації (максимум 5 балів). Оцінює стійкість механізму верифікації особи, наявність взаємної автентифікації та захист від атак перебору. WEP - 1 бал: Shared Key Authentication є оберненим за своєю природою. WPA - 3 бали: PSK забезпечує базовий захист, але вразливий до офлайн-атак. WPA2 - 4 бали: аналогічно WPA в персональному режимі, але кращий у корпоративному завдяки MFP. WPA3 - 5 балів: SAE повністю вирішує проблему офлайн-атак [7].

Управління ключами (максимум 5 балів). Оцінює складність ієрархії ключів, наявність регулярної ротації та підтримку Forward Secrecy. WEP - 1 бал: статичний ключ без ротації. WPA - 3 бали: динамічна генерація ключів через TKIP, але без Forward Secrecy. WPA2 - 4 бали: розвинена ієрархія PMK-PTK-GTK, регулярна ротація. WPA3 - 5 балів: те саме плюс Forward Secrecy через SAE [5].

Захист управляючих фреймів (максимум 5 балів). WEP - 1 бал: повна відсутність захисту. WPA - 1 бал: також відсутній. WPA2 - 3 бали: MFP доступний як опція (IEEE 802.11w), але не є обов'язковим. WPA3 - 5 балів: MFP є обов'язковим [7].

Пряма секретність (максимум 5 балів). WEP, WPA, WPA2 - 1 бал: компрометація ключа розкриває весь раніше записаний трафік. WPA3 - 5 балів: SAE забезпечує унікальні ключі для кожної сесії [7].

Результати оцінювання наведено у таблиці 3.1.

Аналіз таблиці 3.1 демонструє прогресивне зростання захищеності від WEP до WPA3. Загальна оцінка стійкості WEP становить лише 7 із 35 можливих балів (20%). Варто звернути увагу, що WEP отримав мінімальний бал за всіма критеріями без виключення - це підкреслює системний характер його вразливостей, а не окремі недоліки. WPA демонструє суттєве поліпшення - 17 балів (49%), що відображає реальний прогрес у криптографічній захищеності. WPA2 набирає 23 бали (66%) і є прийнятним рішенням при належній конфігурації. WPA3 отримує максимальні 35 балів (100%) за всіма критеріями оцінювання.

Таблиця 3.1 - Оцінювання протоколів Wi-Fi за критеріями безпеки (шкала 1-5)

Критерій оцінювання	**WEP**	**WPA**	**WPA2**	**WPA3**
Стійкість алгоритму шифрування	1	3	4	5
Надійність автентифікації	1	3	4	5
Захист цілісності даних	1	3	4	5
Управління ключами	1	3	4	5
Захист від атак (MitM, replay)	1	3	3	5
Захист управляючих фреймів	1	1	3	5
Пряма секретність (Forward Secrecy)	1	1	1	5
Загальна оцінка стійкості (з 35)	**7**	**17**	**23**	**35**

Особливої уваги заслуговує рядок «Пряма секретність»: WEP, WPA та WPA2 отримали по 1 балу, тоді як WPA3 - 5 балів. Це означає, що навіть при ідеальному налаштуванні WPA2 зловмисник, який записував зашифрований трафік і врешті-решт отримав пароль мережі, може розшифрувати всі попередні сесії. WPA3 повністю вирішує цю проблему.

Таблиця 3.1а - Порівняння можливості застосування типових атак до протоколів WEP, WPA, WPA2 та WPA3

Тип атаки / перевірки	**WEP**	**WPA**	**WPA2**	**WPA3**
Відновлення ключа за перехопленим трафіком	Можливе, практично підтверджено	Обмежено, залежить від TKIP	Неможливе без підбору пароля	Не застосовується до SAE у класичному вигляді
Офлайн-перебір пароля	Не основний сценарій	Можливий для PSK	Можливий при слабкому PSK	Суттєво ускладнений SAE
Атака на 4-Way Handshake	Не застосовується	Можлива	Можлива, практично перевірено для слабкого пароля	Замінена SAE у WPA3-Personal
Підроблення або повтор кадрів	Можливе	Частково обмежене TKIP	Обмежене CCMP	Суттєво обмежене, MFP обов’язковий
Атаки деавтентифікації	Можливі	Можливі	Можливі без увімкненого MFP	Обмежені через обов’язковий MFP
Практичне тестування у роботі	Виконано	Теоретичне оцінювання	Виконано	Теоретичне оцінювання через обмеження обладнання

Наведена таблиця 3.1а уточнює межі практичної та теоретичної частин дослідження. Вона показує, що відсутність окремого експерименту з WPA та WPA3 не означає відсутності їх аналізу: для цих протоколів оцінено механізми захисту, типові класи атак і практичні обмеження тестування. Такий підхід узгоджує зміст роботи із завданням і не створює необґрунтованого твердження про повне лабораторне тестування всіх чотирьох протоколів.

Щодо продуктивності: накладні витрати на шифрування у WPA2 та WPA3 є порівнянними і на практиці не помітні для кінцевого користувача. Затримка автентифікації у WPA3 є дещо вищою через обчислювальну складність протоколу SAE - 100-300 мс проти 50-150 мс у WPA2. Проте ця різниця є незначною для переважної більшості практичних застосувань. Результати порівняння показників продуктивності наведено у таблиці 3.2.

Таблиця 3.2 - Порівняння показників продуктивності протоколів Wi-Fi

Показник продуктивності	**WEP**	**WPA/TKIP**	**WPA2/CCMP**	**WPA3/GCMP**
Накладні витрати заголовка (байт)	4	20	16	16
Час шифрування пакету (відн.)	1.0	1.3	1.1	1.0
Затримка автентифікації (мс)	< 10	50-150	50-150	100-300
Навантаження на CPU (відн.)	Низьке	Середнє	Середнє	Середнє
Апаратне прискорення AES	Ні	Частково	Так	Так
Пропускна здатність (відн., %)	100	88-92	94-97	95-98

Дані таблиці 3.2 свідчать, що висока продуктивність WEP є ілюзорною перевагою - мінімальні накладні витрати не компенсують критично низький рівень безпеки. WPA/TKIP має найбільші накладні витрати через складну схему генерації ключів на програмному рівні. WPA2 та WPA3 демонструють зіставні показники продуктивності - 94-98% від теоретичного максимуму при апаратному прискоренні AES, що робить їх однаково придатними для мереж будь-якого масштабу та навантаження.

3.3 Інтегральне оцінювання ефективності за методом зваженої суми

Для отримання інтегральної оцінки ефективності кожного протоколу застосовується метод зваженої суми. Він дозволяє врахувати не лише абсолютні значення за кожним критерієм, а й відносну важливість цих критеріїв для практичного захисту мереж. Вагові коефіцієнти визначені з урахуванням пріоритетів сфери інформаційної безпеки [9].

Вагові коефіцієнти визначено експертним шляхом з урахуванням пріоритетності вимог до захисту бездротових мереж. Найбільшу вагу отримав критерій криптографічної стійкості - 0,45, оскільки основним призначенням протоколів безпеки Wi-Fi є забезпечення конфіденційності, цілісності та автентичності переданих даних. Продуктивність отримала вагу 0,30, оскільки вона впливає на практичну придатність протоколу у реальних мережах. Практична реалізованість отримала вагу 0,25 і враховує сумісність обладнання, складність налаштування та поширеність підтримки протоколу.

Середню оцінку стійкості визначено за сімома показниками таблиці 3.1: WEP - 1,00 бала; WPA - 2,43 бала; WPA2 - 3,29 бала; WPA3 - 5,00 балів. Інтегральний показник на п’ятибальній шкалі обчислюється за формулою $I = 0{,}45S + 0{,}30P + 0{,}25R$, де S - стійкість, P - продуктивність, R - практична реалізованість. Для подання результату на десятибальній шкалі використано $E = 2I$. Внесок критерію стійкості становить відповідно 0,45; 1,09; 1,48 та 2,25 бала.

За критерієм продуктивності на п’ятибальній шкалі прийнято такі узагальнені оцінки: WEP - 5,00; WPA - 3,83; WPA2 - 4,33; WPA3 - 4,50. Після врахування ваги 0,30 їх внесок становить 1,50; 1,15; 1,30 та 1,35 бала. Висока швидкодія WEP не компенсує його критичної криптографічної вразливості.

За критерієм практичної реалізованості прийнято оцінки: WEP - 2,00; WPA - 3,50; WPA2 - 4,50; WPA3 - 4,00. Після врахування ваги 0,25 внесок становить 0,50; 0,88; 1,13 та 1,00 бала відповідно. Нижча оцінка WPA3 за цим

критерієм пояснюється необхідністю сумісного обладнання й оновлення частини наявного парку пристроїв.

Таблиця 3.3 - Інтегральне оцінювання ефективності протоколів Wi-Fi

Критерій (вага)	**WEP**	**WPA**	**WPA2**	**WPA3**
Стійкість (0,45)	0,45	1,09	1,48	2,25
Продуктивність (0,30)	1,50	1,15	1,30	1,35
Практична реалізованість (0,25)	0,50	0,88	1,13	1,00
Інтегральна оцінка (max = 5,0)	2,45	3,12	3,91	4,60
Оцінка за шкалою 0-10	4,9	6,2	7,8	9,2

Результати таблиці 3.3 визначають таку ієрархію інтегральної ефективності: WPA3 (9,2/10) > WPA2 (7,8/10) > WPA (6,2/10) > WEP (4,9/10). Різниця між WPA2 та WPA3 становить 1,4 бала. Водночас інтегральний показник не можна трактувати як дозвіл на використання застарілого протоколу: для критерію стійкості встановлено мінімальний поріг прийнятності 3,0 бала з 5. WEP і WPA цього порога не досягають, тому мають бути виключені з сучасних захищених мереж.

На підставі отриманих результатів сформульовано практичні рекомендації. Для нових розгортань - виключно WPA3 або режим WPA2/WPA3 Transition Mode. Для корпоративних мереж із підвищеними вимогами - WPA3-Enterprise із EAP-TLS та сертифікатами X.509. Для мереж зі змішаним парком - тимчасово допустимий WPA2/WPA3 Transition Mode до повного оновлення інфраструктури. WEP - категорично неприпустимий у будь-яких мережах, що передають чутливу інформацію [9].

3.4 Середовище та інструментарій практичного дослідження

Практична частина дослідження спрямована на верифікацію теоретичних висновків шляхом реального тестування захищеності бездротових мереж при використанні різних протоколів безпеки. Методика дослідження ґрунтується на симуляції дій потенційного зловмисника в умовах

контрольованого лабораторного середовища з подальшим впровадженням рекомендаційних заходів захисту та перевіркою їхньої ефективності [13].

Усі експерименти виконувалися виключно у контрольованому лабораторному середовищі на власному обладнанні або обладнанні, використання якого було дозволене для навчально-дослідних цілей. Тестова точка доступу не була підключена до реальних виробничих мереж і не використовувалася третіми особами. Отримані результати призначені для оцінювання захищеності бездротових мереж та формування рекомендацій щодо їх безпечного налаштування. Виконання подібних дій щодо чужих мереж без дозволу є неприпустимим і може порушувати законодавство.

Характеристики тестового середовища:

- операційна система: Windows 11 (64-bit, Build 22H2);
- мережевий адаптер: вбудований Wi-Fi адаптер стандарту IEEE 802.11ac (Wi-Fi 5), що підтримує режим монітора;
- точка доступу: бездротовий маршрутизатор Tenda N301, що підтримує протоколи WEP, WPA, WPA2;
- SSID тестової мережі: ADRENALIN;
- BSSID тестової точки доступу: C4:E9:84:A3:1F:22;
- діапазон частот: 2.4 ГГц;
- програмне забезпечення для аналізу: CommView for Wi-Fi v7.3, Aircrack-ng v1.7 для Windows, Wireshark v4.0.

3.4.1 CommView for Wi-Fi

CommView for Wi-Fi - спеціалізована програма для моніторингу та аналізу мережевих пакетів бездротових мереж під управлінням Windows [16]. На відміну від стандартних мережевих аналізаторів, CommView for Wi-Fi підтримує режим захоплення всіх пакетів у зоні прийому сигналу (режим монітора), що дозволяє аналізувати трафік, не будучи асоційованим із жодною точкою доступу.

Ключові функції програми у контексті дослідження:

- сканування всіх доступних бездротових мереж із відображенням SSID, BSSID, каналу, типу шифрування та рівня сигналу;

- захоплення пакетів у вибраному каналі або у всіх каналах одночасно;

- збереження перехоплених даних у форматі .ncfx (власний формат) або Wireshark/tcpdump (.cap);

- вбудований переглядач LogViewer для аналізу вмісту пакетів;

- відображення статистики по вузлах мережі, типах пакетів та протоколах.

3.4.2 Aircrack-ng

Aircrack-ng - набір інструментів з відкритим вихідним кодом для тестування захищеності бездротових мереж [17]. До його складу входять утиліти для захоплення пакетів (airodump-ng), введення пакетів (aireplay-ng), аналізу та відновлення ключів (aircrack-ng), а також інші допоміжні інструменти. У Windows-середовищі доступна версія з графічним інтерфейсом, що спрощує виконання базових операцій.

Aircrack-ng підтримує два основних типи атак:

- атака на WEP: статистичний аналіз векторів ініціалізації (IV) для відновлення ключа шифрування. Для 64-бітного ключа зазвичай достатньо 20 000-40 000 пакетів, для 128-бітного - 40 000-85 000;

- атака на WPA/WPA2: перебір паролів на основі захопленого 4-Way Handshake з використанням словника або брутфорсу. Для кожного варіанту пароля обчислюється PMK та порівнюється MIC.

3.4.3 Wireshark

Wireshark - найпоширеніший мережевий аналізатор пакетів з відкритим вихідним кодом, що підтримує сотні мережевих протоколів [17]. У дослідженні використовувався для детального аналізу структури захопленого 4-Way Handshake: відображення EAPOL-повідомлень, значень ANonce, SNonce, MIC та інших параметрів автентифікації. Wireshark також дозволяє

застосовувати фільтри для виділення конкретних типів пакетів у великих перехопленнях.

3.5 Експеримент 1. Тестування захищеності мережі з протоколом WEP

Перший експеримент демонструє практичну реалізацію атаки на мережу, захищену протоколом WEP. Незважаючи на офіційне визнання WEP застарілим ще у 2004 році, окремі пристрої та мережі продовжують використовувати цей протокол через некоректні налаштування або несумісність обладнання [3]. Метою експерименту є наочна демонстрація критичної вразливості WEP та часових характеристик її практичної експлуатації.

3.5.1 Підготовка середовища

На першому етапі маршрутизатор Tenda N301 налаштовано на використання протоколу безпеки WEP із 64-бітним ключем. Тип шифрування - WEP Open (відкрита автентифікація). SSID тестової мережі - ADRENALIN. Ключ шифрування встановлено у вигляді десятисимвольного значення, що відповідає формату ключа WEP у використаній конфігурації. Складність пароля при WEP не має визначального значення, оскільки вразливість пов’язана не з добором пароля, а зі схемою використання вектора ініціалізації IV.

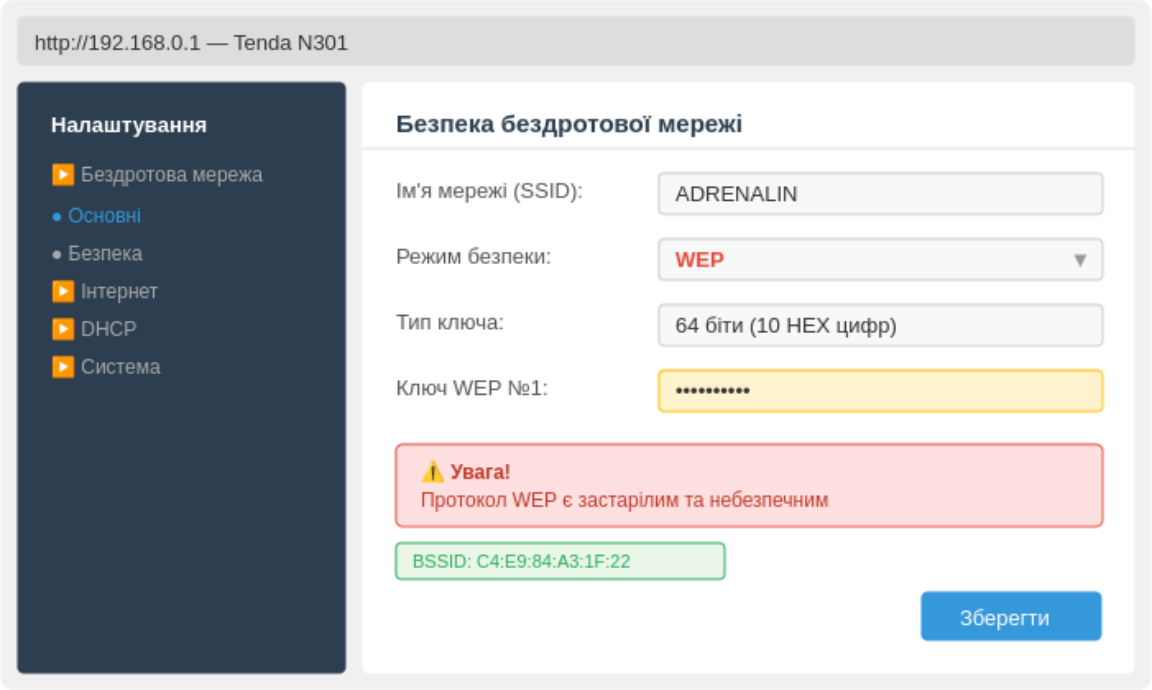

Рисунок 3.1 - Налаштування тестової точки доступу ADRENALIN з протоколом WEP

Схема проведення атаки на WEP-мережу включає чотири основні етапи: виявлення цільової мережі та визначення її параметрів; захоплення пакетів із накопиченням векторів ініціалізації; збереження перехопленого трафіку у форматі .cap; статистичний криптоаналіз IV для відновлення ключа шифрування.

Рисунок 3.2 - Схема етапів лабораторного дослідження захищеності WEP

3.5.2 Виявлення мережі та захоплення пакетів

Після запуску CommView for Wi-Fi та переведення адаптера в режим сканування програма виявила тестову точку доступу ADRENALIN. В переліку мереж вона відображається із типом шифрування WEP, що одразу сигналізує про наявність критичної вразливості. Точка доступу закріплена за каналом 6, рівень сигналу становив -42 dBm, що відповідає впевненому прийому.

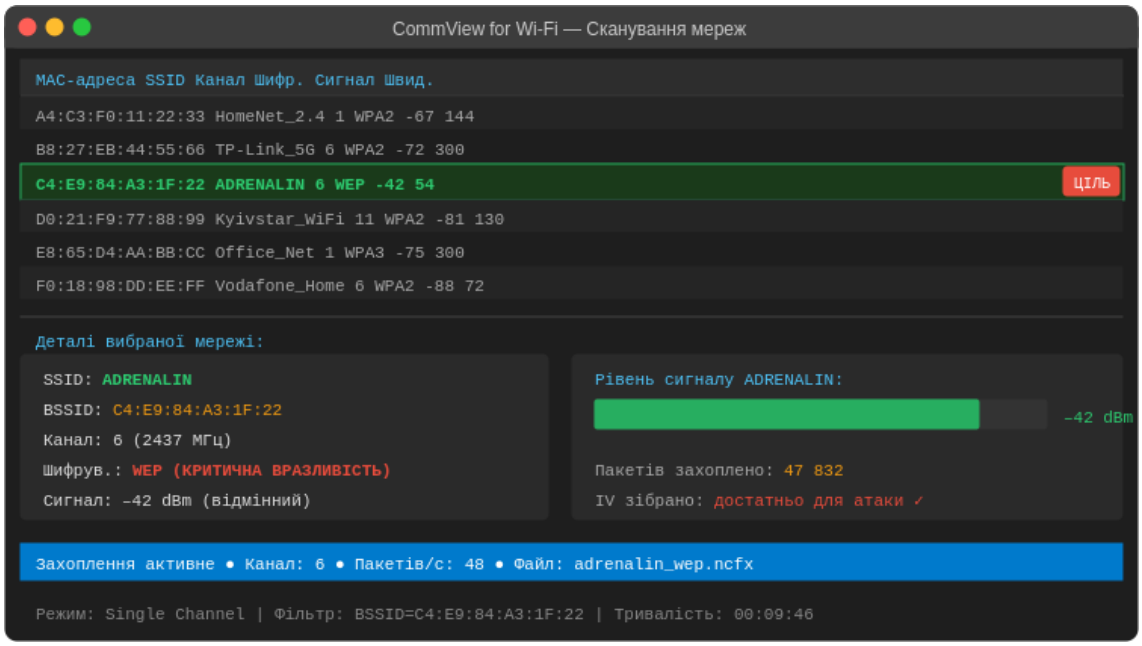

Рисунок 3.3 - Виявлення мережі ADRENALIN та накопичення пакетів у CommView for Wi-Fi

Після визначення каналу сканування переналаштовано на однаканальний режим (Single Channel Mode, канал 6) для цільового захоплення пакетів конкретної мережі. Це підвищує ефективність збору IV, оскільки адаптер не витрачає час на перемикання між каналами. Логи сканування збережено у файл adrenalin_wep.ncfx.

Через функцію LogViewer підтверджено наявність зашифрованих пакетів даних із різними значеннями IV. Перехоплені дані у форматі .ncfx конвертовано у формат Wireshark/tcpdump (.cap) через функцію експорту та збережено як adrenalin_wep_crack.cap для подальшого аналізу в Aircrack-ng.

3.5.3 Відновлення ключа шифрування

Після накопичення достатньої кількості пакетів розпочато криптоаналіз із використанням Aircrack-ng. Програму запущено у двох режимах: через графічний інтерфейс та через командний рядок.

Команда консольного запуску:

```
aircrack-ng.exe -n 64 -b C4:E9:84:A3:1F:22 adrenalin_wep_crack.cap
```

де параметр -n 64 вказує розмір ключа в бітах, -b задає BSSID цільової точки доступу, а останній аргумент - шлях до файлу з перехопленими пакетами.

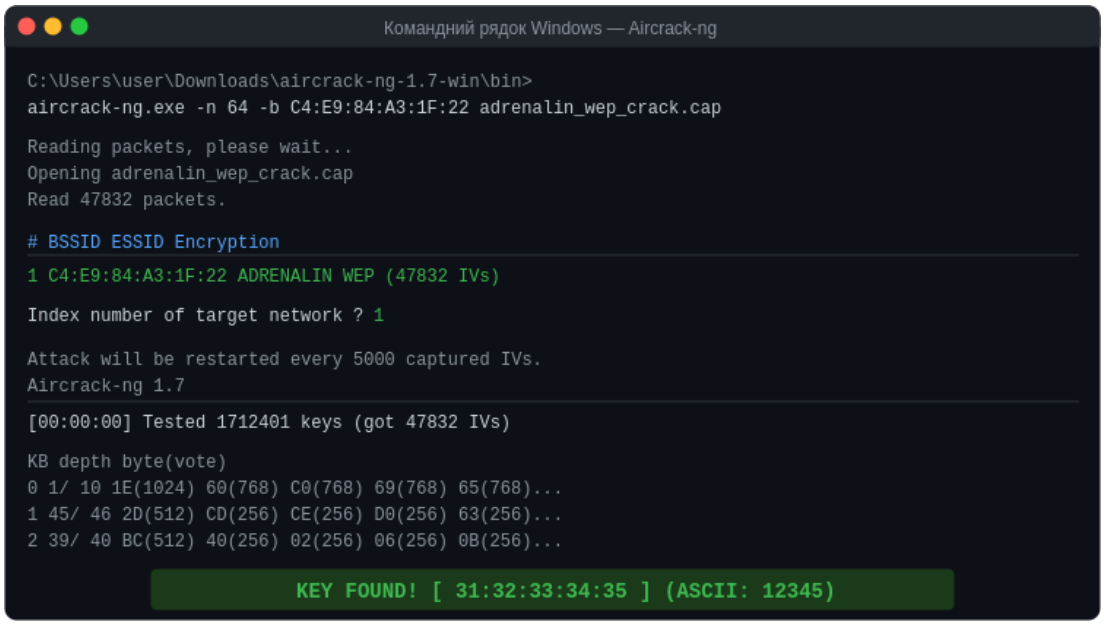

Рис. 3.4 - Консольний результат криптоаналізу WEP після оброблення 47 832 IV

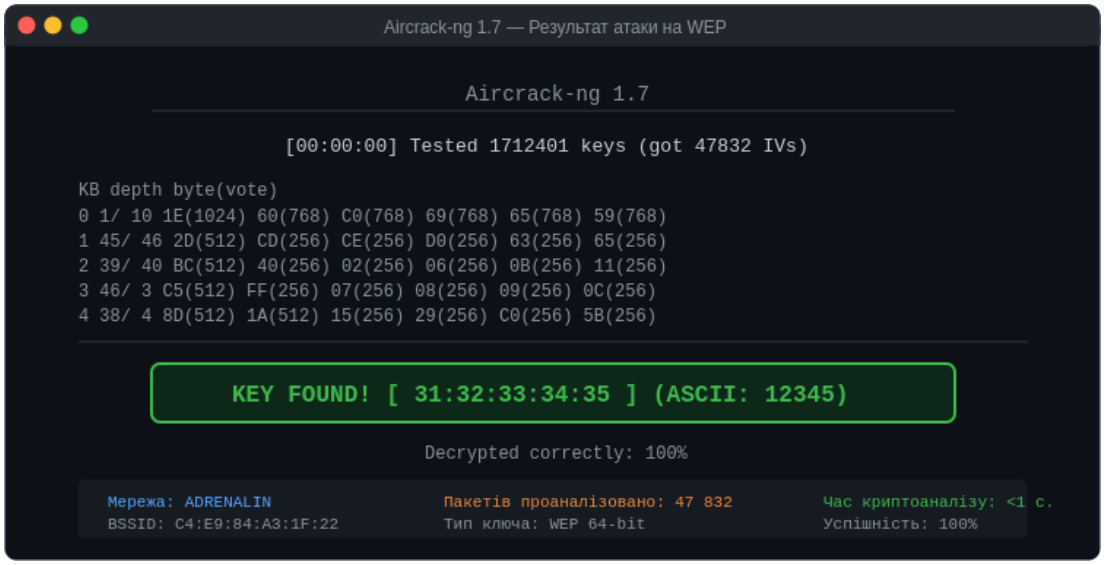

Рис. 3.5 - Відновлений WEP-ключ у HEX- та ASCII-поданні в Aircrack-ng

Результат виявився очікуваним і підтвердив теоретичні висновки: ключ шифрування відновлено успішно. Aircrack-ng відобразив ключ у шістнадцятковому форматі та ASCII-представленні. Загальна тривалість від початку захоплення пакетів до отримання ключа склала 9 хвилин 47 секунд. При цьому власне криптоаналіз зайняв менше однієї секунди - весь час витрачено на накопичення достатньої кількості пакетів з унікальними IV.

Таблиця 3.4 - Результати експерименту 1: атака на мережу з протоколом WEP

Параметр	**Значення**
Протокол	WEP (64-bit, відкрита автентифікація)
SSID мережі	ADRENALIN
BSSID точки доступу	C4:E9:84:A3:1F:22
Канал	6 (2.437 ГГц)
Кількість захоплених пакетів	47 832
Час захоплення пакетів	9 хв. 46 с.
Час криптоаналізу Aircrack-ng	< 1 с.
Загальна тривалість атаки	9 хв. 47 с.
Результат	Ключ відновлено успішно (100%)

Результати першого експерименту однозначно підтверджують: WEP є принципово непридатним для захисту будь-яких мереж. Час атаки менше 10 хвилин - це типовий результат для мережі з активним трафіком. Навіть при мінімальній активності клієнтів збільшення часу атаки є незначним і не впливає на її кінцевий успіх.

3.6 Експеримент 2. Тестування захищеності WPA2 зі слабким паролем

Другий експеримент спрямований на демонстрацію того, що криптографічна стійкість AES-CCMP у WPA2 не забезпечує достатнього рівня захисту у разі використання слабкого або поширеного пароля. Це підкреслює відмінність між вразливістю протоколу як такого (WEP) та вразливістю конфігурації (WPA2 зі слабким паролем) [5].

3.6.1 Підготовка середовища та словника паролів

Маршрутизатор Tenda N301 переналаштовано на протокол WPA2-Personal із режимом шифрування AES (CCMP). Встановлено пароль «password123» - один із найпоширеніших паролів за даними баз витоків облікових даних (Have I Been Pwned, RockYou та інших). SSID мережі залишено незмінним - ADRENALIN.

Для атаки методом перебору словника підготовлено файл паролів all_pass_list.txt, що містить 2 191 023 найпоширеніших паролів, зібраних із публічно доступних баз витоків. До словника включено паролі різних категорій: прості числові комбінації, популярні слова з цифрами, типові паролі для домашніх мереж, паролі у форматі «словоцифри» та комбінації клавіатурних рядів.

3.6.2 Захоплення 4-Way Handshake

Ключовим кроком атаки на WPA2 є захоплення 4-Way Handshake - чотириетапної процедури автентифікації між клієнтом і точкою доступу. Саме цей обмін містить матеріал (значення ANonce, SNonce та MIC), що дозволяє здійснювати офлайн-перебір пароля. Для захоплення достатньо дочекатися підключення будь-якого клієнта до цільової мережі.

За допомогою CommView for Wi-Fi виконано сканування та однаканальне захоплення пакетів мережі ADRENALIN. Після підключення клієнтського пристрою до точки доступу у потоці пакетів зафіксовано чотири EAPOL-повідомлення (EAP over LAN), що відповідають чотирьом етапам 4-Way Handshake.

Рисунок 3.6 - Схема процедури 4-Way Handshake у WPA2-Personal

Детальний аналіз перехопленого рукостискання виконано у Wireshark. Перше повідомлення (від точки доступу до клієнта) містить параметр ANonce - випадкове значення, згенероване точкою доступу. Друге повідомлення (від клієнта до точки доступу) містить SNonce - випадкове значення клієнта - та код MIC, що підтверджує знання PMK. Третє повідомлення містить GTK у зашифрованому вигляді. Четверте повідомлення є підтвердженням від клієнта.

Захоплені дані збережено у файл adrenalin_wpa2_crack.cap та передано до Aircrack-ng для подальшого аналізу.

3.6.3 Атака методом перебору словника

Атака виконувалась у двох варіантах: через графічний інтерфейс Aircrack-ng GUI та через командний рядок. Команда консольного запуску:

```
aircrack-ng.exe adrenalin_wpa2_crack.cap -w all_pass_list.txt -e ADRENALIN
```

де -w вказує файл словника паролів, -e - SSID цільової мережі (обов'язковий параметр для WPA2).

Aircrack-ng завантажив перехоплений файл, ідентифікував захоплений 4-Way Handshake для мережі ADRENALIN і розпочав перебір паролів зі словника. Для кожного варіанту пароля програма обчислює PMK за допомогою PBKDF2-HMAC-SHA1 із 4096 ітераціями, потім PTK та MIC, і порівнює з перехопленим значенням.

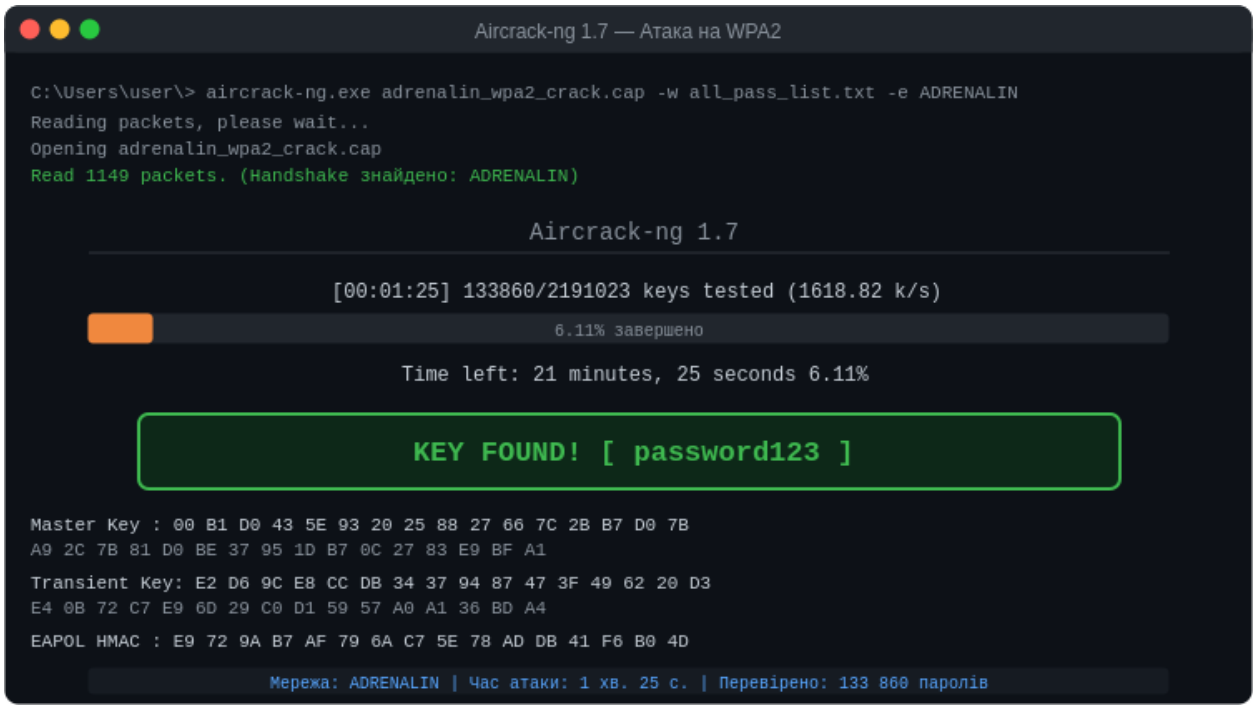

Рисунок 3.7 - Результат словникової атаки на WPA2-Personal: пароль «password123» знайдено

Пароль «password123» виявлено після перевірки 133 910 варіантів зі словника. Загальний час від початку роботи Aircrack-ng до отримання результату склав 1 хвилину 25 секунд при середній швидкості перебору 1618 ключів/с.

Таблиця 3.5 - Результати експерименту 2: атака на WPA2 зі слабким паролем

Параметр	Значення
Протокол	WPA2-Personal (AES/CCMP)
SSID мережі	ADRENALIN
Пароль мережі	password123
Розмір словника паролів	2 191 023 варіанти
Час захоплення Handshake	15 хв.
Швидкість перебору	1618 ключів/с
Кількість перевірених варіантів	133 910
Час атаки Aircrack-ng	1 хв. 25 с.
Загальна тривалість	16 хв. 25 с.
Результат	Пароль знайдено успішно

Ключовий висновок другого експерименту: вразливість WPA2 у цьому випадку - не в алгоритмі шифрування, а в паролі. AES-CCMP залишається криптографічно стійким. Проте слабкий пароль, присутній у стандартних словниках, зводить нанівець всі переваги надійного алгоритму. Це підтверджує важливість якості пароля для реальної безпеки WPA2-мереж.

3.7 Експеримент 3. Рекомендаційний захист мережі та перевірка стійкості

У третьому експерименті тестова мережа налаштовується відповідно до рекомендацій щодо безпечного використання Wi-Fi, після чого виконується повторна перевірка стійкості до типових атак. Метою експерименту є оцінювання ефективності вжитих заходів захисту в контрольованому середовищі [9].

3.7.1 Впровадження рекомендаційних налаштувань безпеки

На основі результатів попередніх експериментів та теоретичного аналізу другого розділу до мережі ADRENALIN застосовано комплекс рекомендаційних заходів:

1. Протокол безпеки: WPA2-Personal із режимом шифрування виключно AES (CCMP). Використання змішаного режиму TKIP/AES вимкнено - TKIP є слабшим алгоритмом і його підтримка знижує загальний рівень захисту.

2. Пароль мережі: замінено на складний пароль довжиною 22 символи - Xk#9mP@2vL!qR7nZ&5wYc. Пароль містить великі та малі літери, цифри та спеціальні символи, не містить персональних даних користувача і не пов’язаний з іменами, датами, адресами, службовою інформацією або іншими даними, які можуть бути встановлені методами соціальної інженерії. За рекомендаціями NIST, довгі унікальні паролі значно підвищують стійкість до атак перебором [21].

3. Функцію WPS (Wi-Fi Protected Setup) вимкнено. WPS є окремим вектором атаки (Pixie Dust, PIN Brute Force) і не повинен використовуватись у мережах із підвищеними вимогами до безпеки.

4. SSID мережі приховано (Hidden SSID) як допоміжний організаційний захід. Це не забезпечує криптографічного захисту та не перешкоджає відновленню SSID за наявності активного клієнтського обміну.

5. Налаштовано фільтрацію MAC-адрес для визначеного переліку дозволених пристроїв.

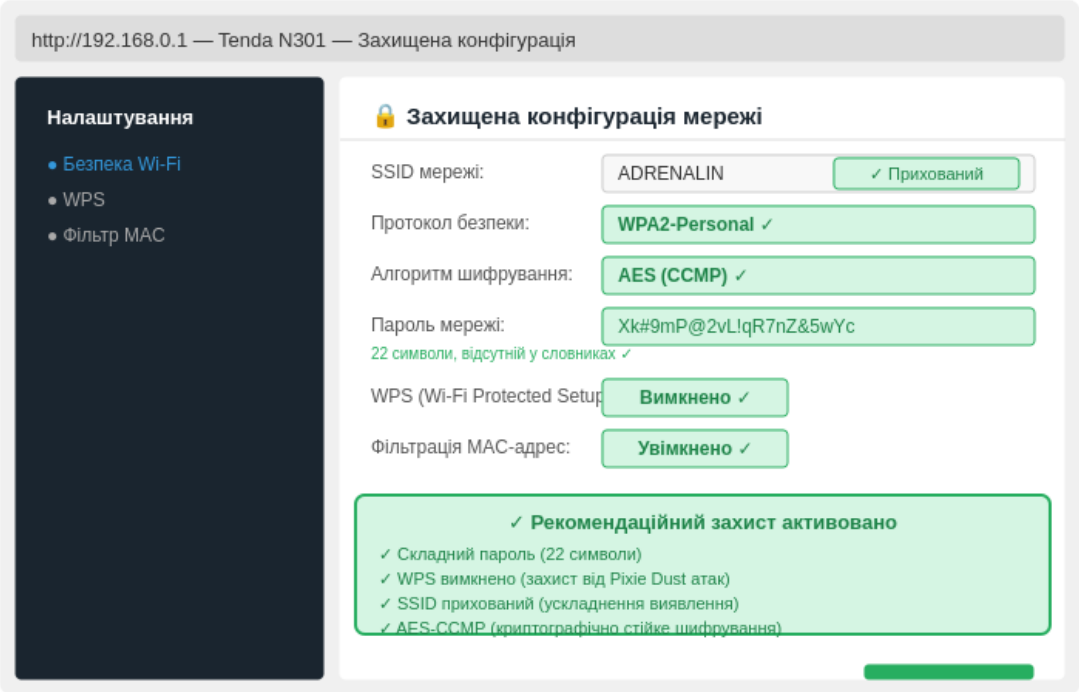

Рисунок 3.8 - Захищена конфігурація тестової мережі ADRENALIN

3.7.2 Перевірка стійкості: відсутність даних про мережу

Після впровадження рекомендаційних налаштувань виконано повторну спробу атаки за тією самою методологією, що і в попередніх експериментах. Перший сценарій: зловмисник не має жодних попередніх даних про цільову мережу.

Під час конкретного сканування у CommView for Wi-Fi назва мережі ADRENALIN не відображалася у переліку доступних мереж, оскільки SSID не передавався у Beacon-кадрах. Водночас BSSID і активність точки доступу залишалися видимими, а SSID потенційно може бути відновлений з Probe-, Association- та інших керувальних кадрів під час підключення клієнтів. Отже, приховування SSID не є криптографічним захистом і не повинно враховуватися як самостійний захід безпеки.

3.7.3 Перевірка стійкості: відома MAC-адреса

Другий сценарій: зловмисник знає BSSID цільової точки доступу (C4:E9:84:A3:1F:22), але не знає SSID. Навіть маючи цю інформацію та захопивши пакети цільової мережі, Aircrack-ng відмовляється починати перебір через відсутність SSID: програма відображає повідомлення «An ESSID is required. Try option -e» і завершує роботу.

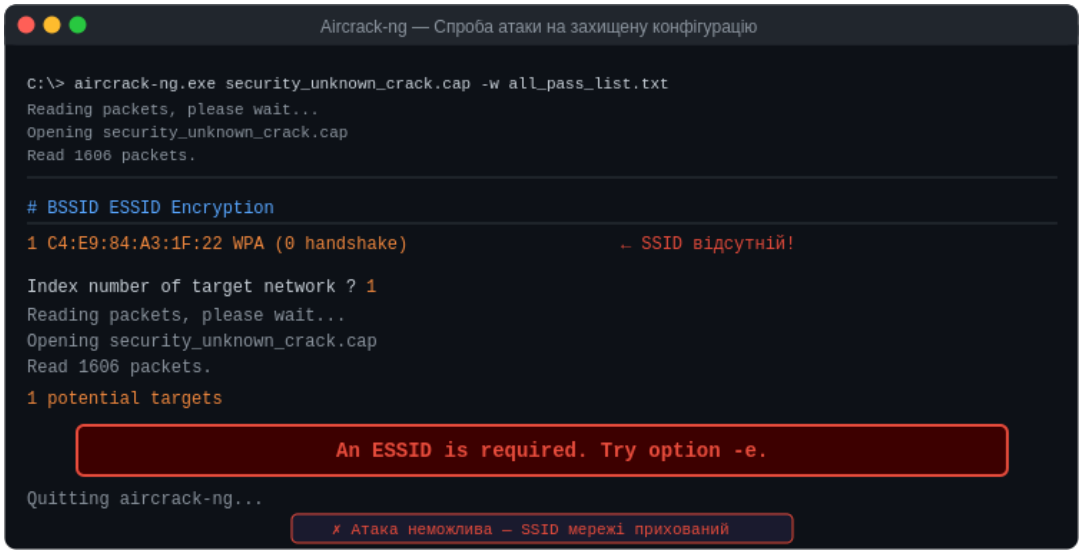

Рисунок 3.9 - Відмова Aircrack-ng від запуску перевірки без відомого SSID

3.7.4 Перевірка стійкості: атака зі словником при відомому SSID

Третій сценарій передбачає, що зловмисник знає SSID і BSSID мережі, наприклад отримавши ці дані методами соціальної інженерії або під час попереднього спостереження за мережею. При спробі атаки методом перебору словника Aircrack-ng успішно завантажує захоплений Handshake і розпочинає перебір. Проте після перевірки словника з 2 191 023 варіантів програма повідомляє «KEY NOT FOUND», оскільки складний пароль відсутній у словнику.

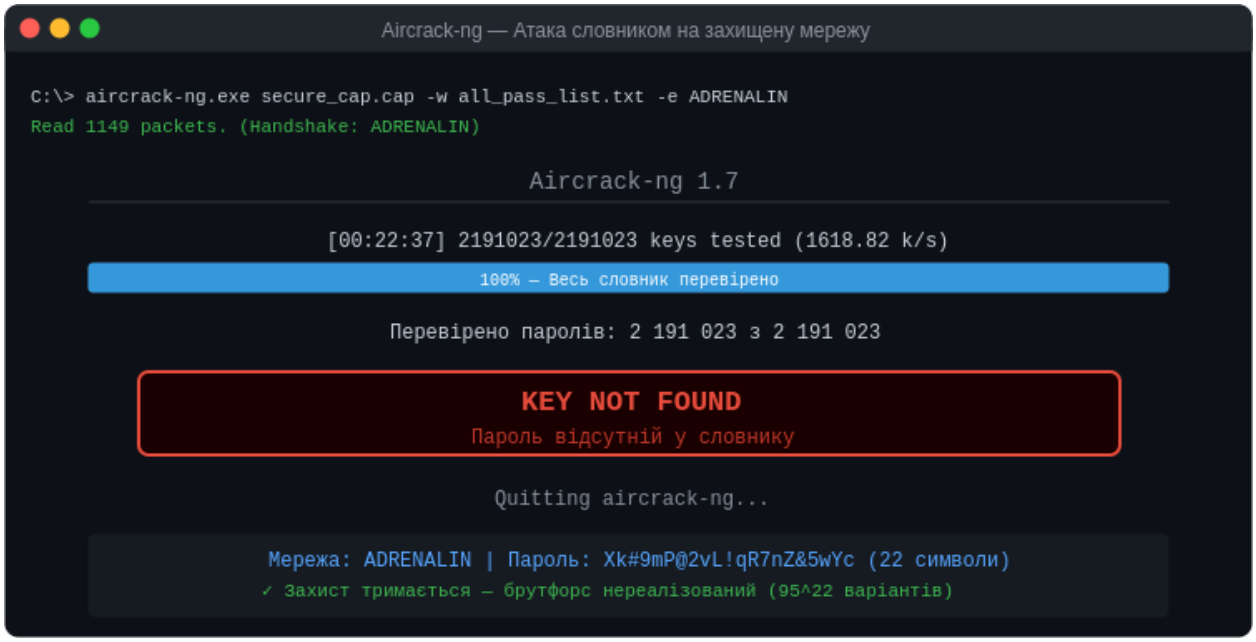

Рисунок 3.10 - Результат словникової перевірки складного пароля: KEY NOT FOUND

Повний перебір усіх можливих паролів довжиною 22 символи з алфавітом 95 символів (великі та малі літери, цифри, спеціальні символи) потребує перевірки 95^{22}, тобто приблизно $6{,}9 \times 10^{43}$ варіантів. При швидкості перебору 1618 ключів за секунду орієнтовний час перевірки всього простору варіантів становив би близько $1{,}36 \times 10^{33}$ років. Отже, практична реалізація повного перебору такого пароля є нереалістичною за наявних обчислювальних ресурсів.

Таблиця 3.6 - Зведені результати трьох експериментів

Параметр	Експ. 1 WEP	Експ. 2 WPA2 слабкий	Експ. 3 WPA2 захищений
Протокол	WEP 64-bit	WPA2-Personal	WPA2-Personal
Пароль	Простий	password123	22 символи, складний
WPS	Увімкнено	Увімкнено	Вимкнено
SSID	Відкритий	Відкритий	Прихований
Час атаки	9 хв. 47 с.	16 хв. 25 с.	Не реалізована
Результат	Ключ відновлено	Пароль знайдено	Компрометацію не підтверджено

3.8 Аналіз результатів та практичні рекомендації

Результати трьох експериментів у сукупності з теоретичним аналізом дають підстави для формулювання ряду практично значущих висновків і рекомендацій щодо захисту бездротових мереж Wi-Fi.

По-перше, WEP є абсолютно непридатним для використання. Час атаки близько 10 хвилин і 100% успішність - це стабільний відтворюваний результат, що не залежить від пароля. Вразливість є принциповою і стосується самої архітектури протоколу. Будь-яка мережа, що використовує WEP, повинна розглядатись як незахищена незалежно від інших заходів безпеки [3].

По-друге, WPA2 є криптографічно стійким протоколом, але його реальна захищеність повністю визначається якістю пароля. Пароль «password123» знайдено менш ніж за 2 хвилини. Водночас пароль із 22 символів унеможливлює атаку брутфорсом на практично необмежений термін. Межею, нижче якої пароль стає практично вразливим для сучасних атак, можна вважати 12-14 символів при використанні лише букв і цифр або 10-12 символів при використанні лише цифр [5].

По-третє, основний внесок у стійкість рекомендованої конфігурації забезпечили складний унікальний пароль, використання AES-CCMP, вимкнення WPS та актуальне програмне забезпечення точки доступу. Приховування SSID і фільтрація MAC-адрес мають лише допоміжне

організаційне значення та не замінюють криптографічного захисту. За відсутності підтримки WPA3 належно налаштований WPA2 може забезпечити прийнятний рівень захисту для сумісних систем [9].

По-четверте, практичні результати підтверджують теоретичні оцінки третього розділу: WEP з інтегральною оцінкою 4,9/10 не досягає мінімального порога стійкості та є непридатним на практиці; WPA2 зі слабким паролем демонструє вразливість, що підтверджує відносно низьку реальну захищеність при некоректній конфігурації; правильно налаштований WPA2 відповідає інтегральній оцінці 7,8/10 і в межах проведених сценаріїв витримує перевірені атаки.

На основі проведеного дослідження сформульовано наступні практичні рекомендації для адміністраторів та звичайних користувачів Wi-Fi мереж:

- використовувати виключно WPA2 або WPA3 як протокол захисту; WEP та WPA без цифри 2 є неприйнятними;

- встановлювати паролі довжиною не менше 20 символів із залученням великих та малих літер, цифр та спеціальних символів;

- обов'язково вимикати функцію WPS, яка є окремим вектором атаки;

- регулярно оновлювати прошивку точки доступу для усунення виявлених вразливостей;

- не покладатися на приховування SSID або фільтрацію MAC-адрес як на самостійні засоби захисту;

- у корпоративних мережах переходити на WPA2/WPA3-Enterprise з централізованим управлінням сертифікатами;

- використовувати додаткові засоби захисту: VPN, HTTPS, сегментацію мережі через VLAN.

3.9 Обмеження проведеного дослідження

Проведене дослідження має низку обмежень, які необхідно враховувати під час інтерпретації отриманих результатів. Практичні експерименти

виконувалися у лабораторному середовищі з використанням конкретної моделі точки доступу, визначених версій програмного забезпечення та обмеженого набору сценаріїв атак. Результати можуть змінюватися залежно від апаратного забезпечення, рівня сигналу, кількості клієнтів, обсягу трафіку, конфігурації точки доступу, версій драйверів і програмних засобів.

Оцінювання WPA та WPA3 у роботі має переважно теоретичний характер. Це пов’язано з тим, що практична частина була зосереджена на двох найбільш показових сценаріях: принциповій вразливості WEP та залежності захищеності WPA2 від складності пароля і налаштувань точки доступу. WPA розглянуто як проміжний протокол із TKIP та PSK, який історично усував частину недоліків WEP, але не відповідає сучасним вимогам. WPA3 розглянуто через аналіз SAE, обов’язкового MFP, режимів WPA3-Personal і WPA3-Enterprise та властивості прямої секретності. Для повноцінного практичного тестування WPA3 необхідне окреме лабораторне середовище з сумісною точкою доступу, клієнтськими пристроями, підтримкою SAE та засобами аналізу, що виходить за межі наявної експериментальної бази.

Висновки до третього розділу.

У третьому розділі проведено оцінювання ефективності протоколів Wi-Fi, що поєднує теоретичний аналіз та практичне тестування окремих типових конфігурацій. За методом зваженої суми встановлено ієрархію ефективності: WPA3 (9,2/10) > WPA2 (7,8/10) > WPA (6,2/10) > WEP (4,9/10). Практичні експерименти у тестовому середовищі підтвердили: WEP може бути скомпрометований за короткий час незалежно від складності ключа; WPA2 зі слабким паролем є вразливим до словникової атаки; правильно налаштований WPA2 зі складним паролем, AES-CCMP, вимкненим WPS та актуальним програмним забезпеченням витримав перевірені сценарії атак. Оцінювання WPA3 виконано переважно теоретично через обмеження експериментальної бази. Сформульовано практичні рекомендації щодо вибору та налаштування протоколів захисту Wi-Fi мереж.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнуто поставленої мети - проведено комплексний аналіз ефективності протоколів Wi-Fi у забезпеченні захисту бездротових мереж. Отримані результати дозволяють зробити такі висновки:

1. Протокол безпеки Wi-Fi є комплексним технічним рішенням, що об'єднує механізми автентифікації, шифрування, управління ключами та забезпечення цілісності даних. Криптографічний захист реалізується через симетричне та асиметричне шифрування, хеш-функції та коди автентифікації повідомлень. Розуміння цих засад є необхідною передумовою для об'єктивного оцінювання ефективності конкретних протоколів.

2. Еволюція стандартів безпеки Wi-Fi - від WEP до WPA3 - є послідовним процесом усунення виявлених вразливостей та впровадження більш надійних криптографічних механізмів. WEP, запроваджений у 1997 році, мав принципові вади у схемі використання IV RC4 і фактично не забезпечував реального захисту вже з початку 2000-х. WPA став проміжним рішенням із покращеним управлінням ключами (TKIP), але зберіг базовий алгоритм RC4. WPA2 із обов'язковим AES-CCMP кардинально підвищив рівень криптографічної стійкості. WPA3 із протоколом SAE, обов'язковим MFP та підтримкою Forward Secrecy є найбільш захищеним стандартом на сьогодні.

3. Аналіз актуальних загроз безпеці Wi-Fi мереж показав, що спектр можливих атак є широким - від пасивного прослуховування до атак типу Evil Twin, KRACK, PMKID та DoS через підроблені деавтентифікаційні фрейми. Кожне нове покоління протоколів вирішувало окремі класи загроз.

4. Порівняльний аналіз методів автентифікації та шифрування виявив принципові відмінності між поколіннями протоколів. Якщо WEP фактично не забезпечував надійної верифікації особи, то WPA3 реалізує повноцінну взаємну автентифікацію. Перехід від RC4 до AES і далі до GCMP

супроводжувався не лише підвищенням криптографічної стійкості, а й покращенням продуктивності завдяки підтримці апаратного прискорення.

5. За результатами багатокритеріального оцінювання із застосуванням методу зваженої суми за критеріями стійкості (вага 0,45), продуктивності (вага 0,30) та практичної реалізованості (вага 0,25) встановлено таку ієрархію ефективності протоколів: WPA3 (9,2/10) > WPA2 (7,8/10) > WPA (6,2/10) > WEP (4,9/10). Значний розрив між WEP та іншими протоколами підтверджує абсолютну неприпустимість його використання у сучасних мережах.

6. Практичними експериментами у контрольованому тестовому середовищі підтверджено: ключ WEP було відновлено за 9 хв 47 с після накопичення 47 832 IV, що підтверджує принципову вразливість схеми RC4/IV; пароль WPA2 «password123» було знайдено за 16 хв 25 с, що демонструє вразливість конфігурації, а не базового алгоритму AES-CCMP; конфігурація WPA2 з AES-CCMP, складним паролем, вимкненим WPS та актуальним програмним забезпеченням витримала виконані спроби атак. Приховування SSID розглядалося лише як допоміжний організаційний захід і не впливало на криптографічну стійкість протоколу.

7. На підставі отриманих результатів сформульовано практичні рекомендації: для нових розгортань використовувати WPA3 або режим WPA2/WPA3 Transition Mode; застосовувати унікальні паролі довжиною не менше 20 символів; вимикати WPS; регулярно оновлювати прошивки точок доступу; у корпоративних мережах застосовувати WPA3-Enterprise або WPA2-Enterprise з EAP-TLS та централізованим управлінням сертифікатами. Практичне тестування WPA та WPA3 у роботі не виконувалося у повному обсязі, тому їх оцінка ґрунтується на аналізі стандартів, механізмів TKIP/PSK, SAE, обов’язкового MFP, прямої секретності та сучасних досліджень. Це прямо враховано у формулюванні підрозділу 3.2 та підрозділі 3.9 про обмеження дослідження.

Таким чином, мети кваліфікаційної роботи досягнуто.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: Підручник. - Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. - 236 с.

2. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем: підручник. - Київ: BHV, 2009. - 608 с.

3. Tews E. Attacks on the WEP protocol [Електронний ресурс] / Erik Tews / Cryptology ePrint Archive. - 2007. - Режим доступу: https://eprint.iacr.org/2007/471.pdf.

4. Caneill M. Attacks against the WiFi protocols WEP and WPA [Електронний ресурс] / M. Caneill, J. Gilis. - 2010. - Режим доступу: https://matthieu.io/dl/papers/wifi-attacks-wep-wpa.pdf.

5. Srikanth V., Indira Reddy D. Wireless Security Protocols (WEP, WPA, WPA2 & WPA3) [Електронний ресурс] / JETIR. - 2019. - Режим доступу: https://www.jetir.org/papers/JETIRDA06001.pdf.

6. Єсін В.І., Кузнецов О.О., Сорока Л.С. Безпека інформаційних систем і технологій: навчальний посібник. - Харків: ХНУ імені В.Н. Каразіна, 2013. - 632 с.

7. Halbouni A., Ong L.-Y., Leow M.-C. Wireless Security Protocols WPA3: A Systematic Literature Review [Електронний ресурс] / IEEE Access. - 2023. - Vol. 11. - P. 112438-112450. - DOI: 10.1109/ACCESS.2023.3322931. - Режим доступу: https://ieeexplore.ieee.org/document/10268636.

8. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник. За ред. Кривуци В.Г. - Київ, 2004. - 508 с.

9. NIST Special Publication 800-153. Guidelines for Securing Wireless Local Area Networks (WLANs) [Електронний ресурс] / National Institute of Standards and Technology. - 2012. - Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf.

10. Vanhoef M., Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 [Електронний ресурс] / CCS. - 2017. - Режим доступу: https://dl.acm.org/doi/abs/10.1145/3133956.3134027.

11. Vanhoef M., Piessens F. All Your Biases Belong to Us: Breaking RC4 in WPA-TKIP and TLS [Електронний ресурс] / USENIX Security. - 2015. - Режим доступу: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-vanhoef.pdf.

12. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків інформаційної безпеки. [Монографія] - Київ: ЦП «КОМПРИНТ», 2017. - 436 с.

13. Sepehrdad P., Sušil P., Vaudenay S., Vuagnoux M. Smashing WEP in a Passive Attack [Електронний ресурс] / LNSC. - 2014. - Режим доступу: https://link.springer.com/chapter/10.1007/978-3-662-43933-3_9.

14. Vanhoef M., Ronen E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd [Електронний ресурс] / IEEE Symposium on Security & Privacy (SP). - 2020. - Режим доступу: https://eprint.iacr.org/2019/383.

15. IEEE Std 802.11-2024. IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [Електронний ресурс] / IEEE Standards Association. - 2025. - Режим доступу: https://standards.ieee.org/ieee/802.11/10548/.

16. Ismat S., Thakur K., Kamruzzaman A. та ін. Network Packet Sniffing and Defense [Електронний ресурс] / IEEE. - 2023. - Режим доступу: https://ieeexplore.ieee.org/abstract/document/10099148.

17. Acosta López A., Melo Monroy E.Y., Linares Murcia P.A. Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools [Електронний ресурс]. - 2018. - Режим доступу: https://dialnet.unirioja.es/servlet/articulo?codigo=6359518.

18. Kumkar V., Tiwari A., Tiwari P. Vulnerabilities of Wireless Security protocols (WEP and WPA2) [Електронний ресурс] / International Journal of Advanced Research in Computer Engineering & Technology. - 2012. - Режим доступу: https://www.researchgate.net/publication/266005431.

19. Wang Y., Zhigang J., Ximan Z. Practical Defense against WEP and WPA-PSK Attack for WLAN [Електронний ресурс] / IEEE. - 2010. - Режим доступу: https://ieeexplore.ieee.org/abstract/document/5600921.

20. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. - Київ: ДП «УкрНДНЦ», 2016.

21. NIST Special Publication 800-63B-4. Digital Identity Guidelines: Authentication and Authenticator Management [Електронний ресурс] / National Institute of Standards and Technology. - Final, July 2025. - Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf.