МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

ЗАХИСТ БЕЗДРОТОВИХ МЕРЕЖ ТА ДОСЛІДЖЕННЯ ЇХ ВРАЗЛИВОСТЕЙ

Виконав: студент групи 1К-22
Спеціальності
123 Комп’ютерна інженерія
Максим БЕЗЧАСНИЙ
Керівник
Майя ЛЮТА

Черкаси 2026

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

Циклова комісія інформаційних, мультимедійних технологій та дизайну

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувачка циклової комісії КІ та ІТ

_____ Наталя ФАЛЬЧЕНКО

(підпис)

«_____» _____2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Безчасному Максиму Сергійовичу

1. Тема кваліфікаційної роботи Захист бездротових мереж та дослідження їх вразливостей

Керівник роботи Люта Майя В'ячеславівна, викладач вищої категорії

затверджені наказом закладу фахової передвищої освіти від «06» жовтня 2025 року № 84/1-у.

2. Строк подання студентом кваліфікаційної роботи 02.06.2026

3. Вихідні дані до кваліфікаційної роботи Архітектура бездротових мереж та стандарти зв'язку; технічні специфікації протоколів шифрування; перелік типових вразливостей бездротових технологій; інструменти аналізу та моніторингу бездротових мереж

4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити) Ознайомлення з сучасними стандартами та принципами забезпечення безпеки в бездротових мережах; аналіз стійкості протоколів шифрування та методів автентифікації до актуальних видів атак; класифікація та аналіз кіберзагроз; огляд та порівняння інструментів для перевірки безпеки мереж; рекомендації щодо покращення безпеки

5. Дата видачі завдання 15.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	14.10.2025	
2	Розділ 1 Огляд основних принципів та технологій безпеки бездротових мереж	09.12.2025	
3	Розділ 2 Аналіз вразливостей та загроз у бездротових мережах	10.03.2026	
4	Розділ 3 Методи дослідження та підвищення безпеки бездротових мереж	28.04.2026	
5	Висновки	12.05.2026	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2026	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2026	
8	Подання кваліфікаційної роботи на затвердження завідувачці циклової комісії (за 7 днів до захисту)	10.06.2026	

Студент _____ Максим БЕЗЧАСНИЙ
(підпис)

Керівник роботи _____ Майя ЛЮТА
(підпис)

АНОТАЦІЯ

Кваліфікаційну роботу присвячено аналізу безпеки сучасних бездротових мереж та виявленню їхніх слабких місць. Основною метою дослідження є оцінка стійкості популярних протоколів шифрування до кібератак та розробка практичних рекомендацій для захисту передачі даних.

У роботі розглянуто стандарти бездротового зв'язку, такі як Wi-Fi та Bluetooth, а також принципи їхньої роботи. Особливу увагу приділено аналізу актуальних загроз: перехопленню трафіку, атакам типу «людина посередині» (MITM) та несанкціонованому доступу до мережі. Обґрунтовано вибір спеціалізованих програмних інструментів, які дозволяють проводити аудит безпеки та виявляти критичні вразливості.

Практична частина роботи включає проведення тестування на проникнення в умовах контрольованої тестової мережі. Це дозволило на прикладі відтворити сценарії можливих атак, перевірити ефективність чинних механізмів захисту та виявити найбільш небезпечні методи взлому. За результатами проведених випробувань сформульовано комплекс заходів для зміцнення безпеки бездротового середовища.

Ключові слова: БЕЗДРОТОВІ МЕРЕЖІ, WI-FI, КІБЕРБЕЗПЕКА, ВРАЗЛИВОСТІ, ПРОТОКОЛИ ШИФРУВАННЯ, ТЕСТУВАННЯ НА ПРОНИКНЕННЯ, ЗАХИСТ ДАНИХ.

ABSTRACT

The qualification work is devoted to the security analysis of modern wireless networks and the identification of their weaknesses. The primary goal of the research is to assess the resilience of popular encryption protocols against cyberattacks and to develop practical recommendations for data transmission protection.

The work examines wireless communication standards, such as Wi-Fi and Bluetooth, along with their operating principles. Special attention is paid to the analysis of current threats: traffic interception, Man-in-the-Middle (MITM) attacks, and unauthorized network access. The selection of specialized software tools that allow for security audits and the detection of critical vulnerabilities is justified.

The practical part of the work includes penetration testing within a controlled test network. This allowed for the replication of potential attack scenarios, testing the effectiveness of existing security mechanisms, and identifying the most dangerous hacking methods. Based on the test results, a set of measures has been formulated to strengthen the security of the wireless environment.

Keywords: WIRELESS NETWORKS, WI-FI, CYBERSECURITY, VULNERABILITIES, ENCRYPTION PROTOCOLS, PENETRATION TESTING, DATA PROTECTION.

ЗМІСТ

ВСТУП

У сучасному світі бездротові мережі стали невід'ємною складовою інформаційно-комунікаційної інфраструктури. Технології Wi-Fi, Bluetooth, LTE та 5G широко використовуються як у побуті, так і в діяльності підприємств, освітніх установ та державних організацій. Завдяки простоті розгортання, мобільності та зручності використання бездротові мережі забезпечують швидкий доступ до інформаційних ресурсів і мережевих сервісів. Разом із тим широке поширення бездротових технологій супроводжується зростанням кількості кіберзагроз, спрямованих на отримання несанкціонованого доступу до мережі, перехоплення даних та порушення конфіденційності інформації.

На відміну від дротових мереж, передавання інформації в бездротовому середовищі здійснюється через радіоканал, що створює додаткові ризики безпеки. Зловмисники можуть здійснювати підбір паролів, перехоплювати мережевий трафік, використовувати вразливості протоколів шифрування або застосовувати методи соціальної інженерії для отримання доступу до мережевих ресурсів.

Актуальність теми полягає в необхідності дослідження сучасних загроз бездротовим мережам, аналізу їх вразливостей та визначення ефективних способів підвищення рівня захисту мережевої інфраструктури. Забезпечення безпеки бездротових мереж є важливою умовою захисту інформаційних ресурсів від несанкціонованого доступу та інших кіберзагроз.

Метою кваліфікаційної роботи є дослідження вразливостей бездротових мереж, аналіз можливих загроз безпеці та розроблення рекомендацій щодо підвищення рівня їх захисту.

Для досягнення поставленої мети необхідно виконати такі завдання:

– розглянути основні принципи функціонування бездротових мереж та їх класифікацію;

– проаналізувати сучасні стандарти бездротового зв’язку та протоколи захисту даних;

– розглянути методи автентифікації та контролю доступу в бездротових мережах;

– дослідити основні вразливості та загрози бездротових мереж;

– проаналізувати способи реалізації атак на бездротові мережі;

– виконати моделювання бездротової мережі в середовищі Cisco Packet Tracer;

– провести аналіз ризиків та оцінити рівень безпеки змодельованої мережі;

– розробити рекомендації щодо підвищення рівня захисту бездротових мереж.

Об’єктом дослідження є процес забезпечення безпеки бездротових комп’ютерних мереж.

Предметом дослідження є методи захисту бездротових мереж, їх вразливості, потенційні загрози та механізми підвищення рівня інформаційної безпеки.

Практичне значення одержаних результатів полягає в дослідженні можливих загроз бездротовим мережам та оцінці ефективності засобів захисту на прикладі змодельованої мережі в середовищі Cisco Packet Tracer. Отримані результати можуть бути використані під час проєктування та налаштування бездротових мереж для підвищення рівня їх захищеності від несанкціонованого доступу, а також у навчальному процесі під час вивчення дисциплін, пов’язаних із комп’ютерними мережами та кібербезпекою.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. У першому розділі розглянуто теоретичні основи безпеки бездротових мереж. Другий розділ присвячено аналізу вразливостей та загроз у бездротовому середовищі. У третьому розділі наведено результати дослідження, оцінку ризиків та рекомендації щодо підвищення рівня захисту бездротових мереж.

Апробація результатів дослідження була здійснена в межах XVIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Тенденції розвитку ІТ-технологій в Україні» [13].

РОЗДІЛ 1 ОГЛЯД ОСНОВНИХ ПРИНЦИПІВ ТА ТЕХНОЛОГІЙ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ

1.1 Поняття та класифікація бездротових мереж

Бездротові мережі сьогодні є одними з найпоширеніших способів передачі інформації між різними пристроями. Вони дозволяють обмінюватися даними без використання кабелів, що робить їх зручними та простими у використанні. Передача інформації у бездротових мережах здійснюється за допомогою радіохвиль або інших технологій бездротового зв'язку. Завдяки цьому користувачі можуть отримувати доступ до мережі Інтернет, локальних ресурсів та різних сервісів незалежно від свого місцезнаходження в межах зони покриття мережі.

Популярність бездротових мереж постійно зростає через активне використання смартфонів, ноутбуків, планшетів та інших мобільних пристроїв. Такі мережі широко використовуються у будинках, офісах, навчальних закладах, підприємствах та громадських місцях. Вони значно спрощують процес підключення пристроїв до мережі та дозволяють швидко організувати доступ до Інтернету без необхідності прокладання великої кількості кабелів.

Основними перевагами бездротових мереж є мобільність користувачів, зручність використання та можливість швидкого розгортання мережевої інфраструктури. Крім цього, бездротові мережі дозволяють легко підключати нові пристрої та розширювати мережу без значних витрат. Проте такі мережі мають і певні недоліки. До них можна віднести можливість перехоплення сигналу сторонніми особами, вплив перешкод на якість зв'язку, зниження швидкості передачі даних при великій кількості підключених користувачів, а також підвищений ризик несанкціонованого доступу до мережі.

Бездротові мережі класифікуються залежно від радіуса дії, сфери використання та технологій передачі даних. Основні типи бездротових мереж наведено у таблиці 1.1.

Таблиця 1.1 – Класифікація бездротових мереж

Тип бездротової мереж	Повна назва	Приклади технологій	Основне призначення	Радіус дії
WLAN	Wireless Local Area Network	Wi-Fi	Організація локальної мережі в будинках, офісах, навчальних закладах	До 100 м
WPAN	Wireless Personal Area Network	Bluetooth, NFC	З'єднання персональних пристроїв між собою	До 10-30 м
WMAN	Wireless Metropolitan Area Network	WiMAX	Забезпечення бездротового зв'язку в межах міста або району	До кількох десятків км
WWAN	Wireless Wide Area Network	3G, 4G LTE, 5G	Мобільний зв'язок та доступ до Інтернету на великих територіях	Сотні кілометрів

Найбільш поширеним видом бездротових мереж є WLAN, оскільки саме технологія Wi-Fi використовується для підключення більшості сучасних пристроїв до мережі Інтернет [1].

1.2 Стандарти бездротового зв'язку (Wi-Fi, Bluetooth, LTE, 5G)

Сучасні бездротові мережі працюють на основі різних стандартів зв'язку, які визначають способи передачі даних, швидкість роботи мережі, радіус покриття та рівень захисту інформації. Розвиток бездротових технологій дозволив забезпечити швидкий обмін даними між пристроями, доступ до мережі Інтернет та підтримку великої кількості користувачів одночасно. Найбільш поширеними стандартами бездротового зв'язку є Wi-Fi, Bluetooth, LTE та 5G.

Технологія Wi-Fi є найпоширенішим стандартом бездротових локальних мереж. Вона використовується у будинках, офісах, навчальних закладах та громадських місцях для забезпечення доступу до Інтернету та локальної мережі.

Робота Wi-Fi базується на стандартах IEEE 802.11. Основними перевагами цієї технології є висока швидкість передачі даних, простота налаштування та можливість підключення великої кількості пристроїв. Сучасні стандарти Wi-Fi забезпечують стабільне з'єднання та підтримують високі швидкості передачі інформації, що дозволяє використовувати потокове відео, онлайн-ігри та хмарні сервіси.

Bluetooth є стандартом бездротового зв'язку малого радіуса дії, який використовується для обміну даними між різними пристроями. Найчастіше ця технологія застосовується для підключення навушників, клавіатур, комп'ютерних мишок, смартфонів та інших мобільних пристроїв. Основною перевагою Bluetooth є низьке енергоспоживання та простота використання. Радіус дії Bluetooth зазвичай становить до 10 метрів, хоча сучасні версії технології можуть працювати і на більшій відстані.

LTE (Long Term Evolution) є стандартом мобільного зв'язку четвертого покоління, який забезпечує високошвидкісний доступ до Інтернету. Технологія LTE використовується мобільними операторами для передачі даних у мережах 4G. Основними перевагами LTE є висока швидкість передачі інформації, стабільне з'єднання та можливість роботи на великих територіях. Завдяки LTE користувачі можуть переглядати відео високої якості, користуватися онлайн-сервісами та швидко передавати великі обсяги даних.

Технологія 5G є новим поколінням мобільного зв'язку, яке поступово впроваджується у різних країнах світу. Основною особливістю 5G є значно вища швидкість передачі даних порівняно з попередніми поколіннями мереж. Крім цього, 5G забезпечує мінімальні затримки сигналу та підтримку великої кількості підключених пристроїв одночасно. Це дозволяє використовувати технологію у сферах автоматизації, Інтернету речей, системах «розумного міста», автономному транспорті та інших сучасних інформаційних системах.

Кожен із розглянутих стандартів має свої особливості, переваги та сферу використання. Wi-Fi і Bluetooth переважно застосовуються для локального обміну даними між пристроями, тоді як LTE та 5G використовуються для

забезпечення мобільного зв’язку та доступу до мережі Інтернет на великих територіях. Разом із розвитком стандартів бездротового зв’язку зростають і вимоги до захисту інформації, тому забезпечення безпеки таких мереж є важливим завданням сучасних інформаційних технологій.

Технологія Wi-Fi розвивалася протягом багатьох років, і сьогодні існує велика кількість стандартів IEEE 802.11, кожен із яких має власні характеристики щодо частотного діапазону, пропускної здатності та методів передачі даних. Розуміння особливостей цих стандартів важливе для правильного вибору обладнання та налаштування параметрів безпеки. Порівняльну характеристику основних стандартів Wi-Fi наведено у таблиці 1.2.

Таблиця 1.2 – Порівняльна характеристика стандартів IEEE 802.11

Стандарт	Рік прийняття	Частота (ГГц)	Макс. швидкість	Комерційна назва
802.11b	1999	2,4	11 Мбіт/с	Wi-Fi 1
802.11g	2003	2,4	54 Мбіт/с	Wi-Fi 3
802.11n	2009	2,4 / 5	600 Мбіт/с	Wi-Fi 4
802.11ac	2014	5	6,93 Гбіт/с	Wi-Fi 5
802.11ax	2019	2,4 / 5 / 6	9,6 Гбіт/с	Wi-Fi 6/6E
802.11be	2024	2,4 / 5 / 6	до 46 Гбіт/с	Wi-Fi 7

З точки зору безпеки, важливим аспектом є те, що старіші стандарти (802.11b, 802.11g) є більш вразливими до атак через обмежені можливості шифрування та меншу кількість доступних каналів зв’язку. Сучасні стандарти Wi-Fi 6 та Wi-Fi 7 підтримують обов’язкове використання WPA3 та вдосконалені механізми захисту від атак на відмову в обслуговуванні. Вибір відповідного стандарту Wi-Fi є важливим кроком при проєктуванні захищеної бездротової мережі [5].

1.3 Основні протоколи шифрування (WEP, WPA, WPA2, WPA3)

Одним із найважливіших елементів захисту бездротових мереж є використання протоколів шифрування. Оскільки передача даних у бездротових мережах здійснюється через радіосигнал, інформація може бути перехоплена сторонніми особами. Для запобігання несанкціонованому доступу та захисту

конфіденційних даних використовуються спеціальні протоколи шифрування, які забезпечують кодування інформації під час її передачі мережею.

Протоколи шифрування призначені для захисту даних від перехоплення, підробки та несанкціонованого доступу. Вони забезпечують конфіденційність інформації, автентифікацію користувачів та контроль цілісності даних. З розвитком бездротових технологій протоколи захисту також вдосконалювалися, оскільки старі методи шифрування з часом ставали вразливими до атак.

Одним із перших протоколів захисту бездротових мереж був WEP (Wired Equivalent Privacy). Основною метою WEP було забезпечення рівня безпеки, подібного до дротових мереж. Проте цей протокол мав значні недоліки у механізмах шифрування та швидко став вразливим до злому. Через слабкий алгоритм захисту зловмисники могли отримати пароль мережі за відносно короткий час, тому сьогодні використання WEP вважається небезпечним [3].

Для усунення недоліків WEP був створений протокол WPA (Wi-Fi Protected Access). У WPA були покращені механізми автентифікації та шифрування даних. Протокол використовував динамічні ключі шифрування, що значно підвищило рівень безпеки мережі. WPA став тимчасовим рішенням до появи більш сучасного стандарту WPA2.

Протокол WPA2 тривалий час залишався основним стандартом захисту бездротових мереж. Він використовує більш надійний алгоритм шифрування AES, який забезпечує високий рівень безпеки даних. WPA2 широко застосовується у домашніх та корпоративних мережах і забезпечує захист від більшості типових атак. Незважаючи на високу надійність, WPA2 також має певні вразливості, особливо при використанні слабких паролів.

Найсучаснішим стандартом захисту бездротових мереж є WPA3. Він забезпечує покращений рівень захисту інформації та має більш стійкі механізми автентифікації. WPA3 краще захищає мережу від підбору паролів та забезпечує безпечніше з’єднання навіть при використанні простих паролів користувачами. Основні характеристики протоколів шифрування наведено у таблиці 1.3.

Таблиця 1.3 – Порівняння протоколів шифрування бездротових мереж

Протокол	Рівень безпеки	Основний алгоритм	Основні особливості
WEP	Низький	RC4	Застарілий протокол, легко піддається злому
WPA	Середній	TKIP	Покращений захист порівняно з WEP
WPA2	Високий	AES	Найпоширеніший стандарт захисту Wi-Fi мереж
WPA3	Дуже високий	AES, SAE	Покращений захист від підбору паролів та сучасних атак

Таким чином, розвиток протоколів шифрування дозволив значно підвищити рівень безпеки бездротових мереж. Сучасні стандарти захисту забезпечують конфіденційність переданих даних та ускладнюють несанкціонований доступ до мережі [3].

1.4 Методи автентифікації та контролю доступу

Одним із важливих елементів захисту бездротових мереж є автентифікація користувачів та контроль доступу до мережевих ресурсів. Оскільки бездротові мережі передають інформацію через радіосигнал, існує ризик підключення сторонніх осіб до мережі без дозволу власника. Саме тому для забезпечення безпеки використовуються різні методи перевірки користувачів та обмеження доступу до мережі.

Автентифікація – це процес перевірки користувача або пристрою перед наданням доступу до мережі. Основною метою автентифікації є підтвердження того, що користувач має право підключатися до бездротової мережі. Контроль доступу, у свою чергу, дозволяє обмежувати можливості користувачів та запобігати несанкціонованому використанню мережі.

Одним із найпростіших методів захисту є використання пароля доступу до Wi-Fi мережі. Для підключення до мережі користувач повинен ввести правильний пароль, який використовується для шифрування та автентифікації. Надійність такого методу залежить від складності пароля. Використання простих або коротких паролів значно підвищує ризик їх підбору зловмисниками.

Ще одним методом контролю доступу є фільтрація MAC-адрес. Кожен мережевий пристрій має унікальну MAC-адресу, за допомогою якої його можна ідентифікувати у мережі. Адміністратор може створити список дозволених пристроїв, яким буде надано доступ до мережі.

У корпоративних мережах часто використовується автентифікація за допомогою сервера RADIUS. Такий підхід дозволяє централізовано перевіряти користувачів та контролювати їх доступ до мережі. Для автентифікації можуть використовуватися логіни, паролі, сертифікати безпеки або інші методи підтвердження особи користувача. Використання RADIUS забезпечує вищий рівень безпеки порівняно зі звичайним паролем Wi-Fi.

Сучасні бездротові мережі також підтримують багатофакторну автентифікацію. У такому випадку для підтвердження особи користувач повинен пройти декілька етапів перевірки, наприклад ввести пароль та підтвердити вхід через мобільний пристрій. Основні методи автентифікації та контролю доступу в бездротових мережах зображено на рисунку 1.1.

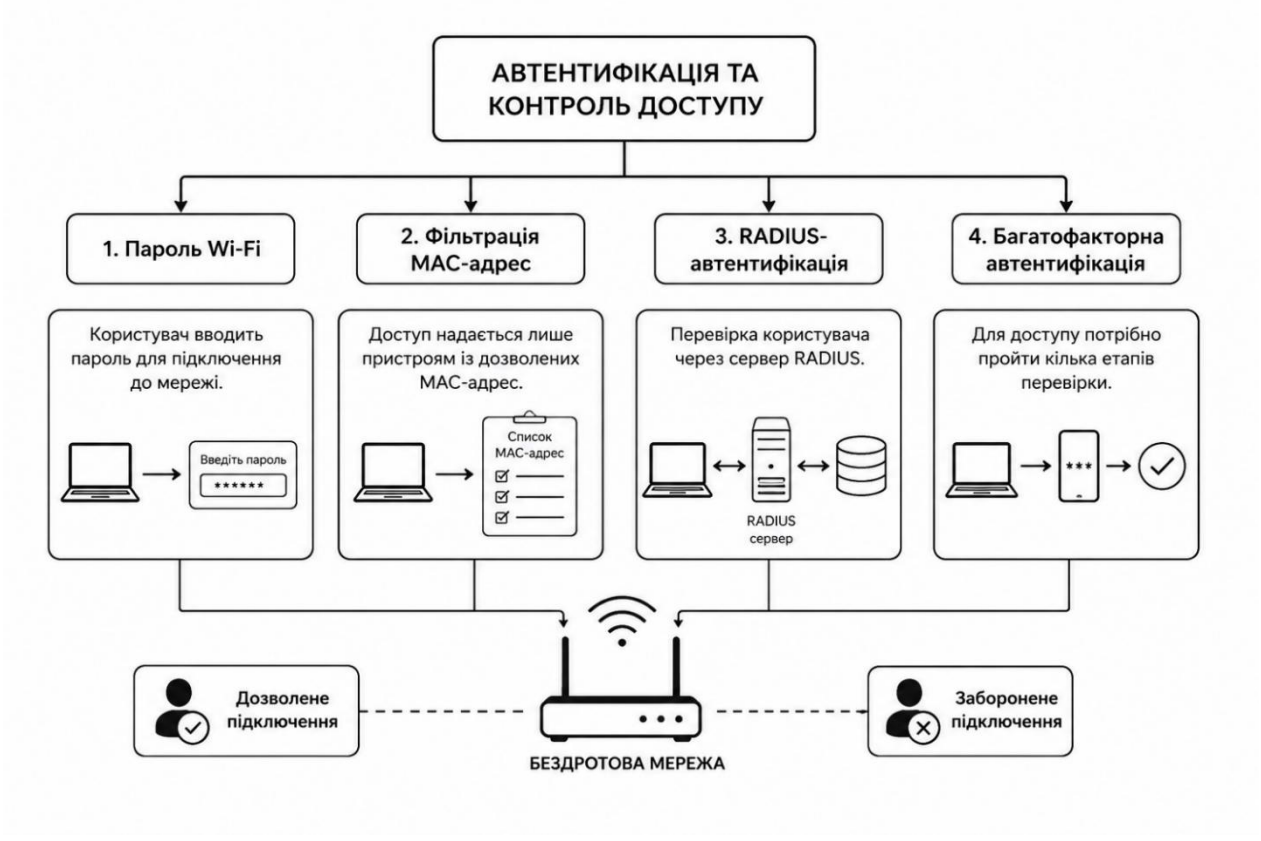

Рисунок 1.1 – Методи автентифікації та контролю доступу

Отже, використання методів автентифікації та контролю доступу є необхідною умовою забезпечення безпеки бездротових мереж. Сучасні технології дозволяють значно знизити ризик несанкціонованого підключення та підвищити рівень захисту інформації. Для ефективного захисту мережі рекомендується використовувати складні паролі, сучасні методи автентифікації та додаткові засоби контролю доступу.

Порівняльний аналіз методів автентифікації дозволяє визначити їхні переваги та недоліки з точки зору рівня захисту, зручності використання та вартості впровадження. Вибір конкретного методу залежить від масштабу мережі, вимог до безпеки та наявних ресурсів. Основні характеристики методів автентифікації наведено у таблиці 1.4.

Таблиця 1.4 – Порівняльна характеристика методів автентифікації

Метод автентифікації	Рівень безпеки	Складність впровадження	Типове застосування
Пароль (PSK)	Середній	Низька	Домашні мережі
Фільтрація MAC-адрес	Низький (як доповнення)	Низька	Малі офіси
RADIUS/802.1X	Високий	Висока	Корпоративні мережі
Багатофакторна автентифікація (MFA)	Дуже високий	Середня	Критичні системи, банківські установи
Цифрові сертифікати (PKI)	Дуже високий	Дуже висока	Великі корпорації, державні установи

Стандарт IEEE 802.1X є одним із найбільш ефективних механізмів контролю доступу до мережі. Він забезпечує централізовану автентифікацію пристроїв на основі ролей та облікових даних користувачів. Протокол EAP (Extensible Authentication Protocol), що використовується разом із 802.1X, підтримує різні методи перевірки особи: від паролів до цифрових сертифікатів. Завдяки цьому адміністратори отримують гнучкі можливості налаштування політик доступу залежно від типу пристрою та ролі користувача.

Окремої уваги заслуговує технологія WPA3-Enterprise, яка поєднує переваги стандарту WPA3 із корпоративними механізмами автентифікації. У цьому режимі кожен користувач має власні облікові дані для доступу до мережі,

що виключає ризик розкриття спільного пароля. Шифрування трафіку здійснюється із застосуванням 192-бітних ключів, що відповідає вимогам державних стандартів безпеки. Ця технологія рекомендована для захисту мереж фінансових установ, медичних закладів та інших організацій, що обробляють конфіденційні дані.

Важливо також зазначити, що ефективність будь-якого методу автентифікації значною мірою залежить від правильного налаштування мережевого обладнання та дотримання користувачами правил інформаційної безпеки. Навіть найсучасніший метод захисту не дасть бажаного результату, якщо пристрої не оновлюються або якщо користувачі передають свої облікові дані третім особам. Тому організація навчання та підвищення обізнаності користувачів є невід’ємною частиною комплексної системи захисту бездротових мереж [2].

РОЗДІЛ 2 АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА ЗАГРОЗ У БЕЗДРОТОВИХ МЕРЕЖАХ

2.1 Типові вразливості бездротових мереж

Бездротові мережі є зручним та популярним способом передачі інформації, проте через особливості своєї роботи вони мають значну кількість вразливостей. На відміну від дротових мереж, де для підключення необхідний фізичний доступ до кабелю, бездротові мережі передають дані через радіосигнал, який може бути перехоплений будь-яким пристроєм у межах зони покриття. Саме тому питання безпеки бездротових мереж є дуже актуальним.

Однією з основних вразливостей бездротових мереж є використання слабких або стандартних паролів. Багато користувачів встановлюють прості паролі, які легко підібрати за допомогою спеціальних програм. Також часто залишаються заводські налаштування маршрутизатора, що значно спрощує отримання несанкціонованого доступу до мережі.

Ще однією поширеною проблемою є використання застарілих протоколів шифрування, зокрема WEP. Цей протокол має серйозні недоліки у системі захисту, через що пароль мережі може бути отриманий за короткий проміжок часу. Навіть сучасніші протоколи можуть бути вразливими у випадку неправильного налаштування мережі або використання ненадійних паролів.

Суттєвою вразливістю є відкритість радіосигналу. Будь-який користувач у межах дії мережі може спробувати перехопити мережевий трафік або виконати аналіз переданих даних. Якщо мережа недостатньо захищена, це може призвести до викрадення конфіденційної інформації, логінів, паролів та інших даних користувачів.

Також небезпеку становлять фальшиві точки доступу. Зловмисники можуть створювати підроблені Wi-Fi мережі з назвами, схожими на справжні. Користувачі підключаються до таких мереж, після чого зловмисник отримує можливість перехоплювати передану інформацію або перенаправляти користувача на шкідливі ресурси.

Ще однією проблемою є відсутність регулярного оновлення програмного забезпечення мережевого обладнання. Маршрутизатори та точки доступу можуть містити вразливості, які виробники усувають у нових версіях прошивки. Якщо користувач не оновлює обладнання, зловмисники можуть використати відомі помилки для отримання доступу до мережі.

Крім цього, бездротові мережі можуть бути вразливими до атак типу відмови в обслуговуванні (DoS). Під час такої атаки мережа перевантажується великою кількістю запитів, через що користувачі втрачають можливість нормально користуватися Інтернетом або іншими мережевими ресурсами.

Таким чином, бездротові мережі мають різні вразливості, які можуть призвести до витоку інформації, несанкціонованого доступу або порушення роботи мережі. Для забезпечення належного рівня безпеки необхідно використовувати сучасні протоколи шифрування, складні паролі, регулярно оновлювати мережеве обладнання та контролювати підключення до мережі.

2.2 Атаки на протоколи шифрування

Протоколи шифрування є основним засобом захисту бездротових мереж від несанкціонованого доступу та перехоплення інформації. Вони забезпечують кодування даних під час передачі між пристроями та точкою доступу. Проте навіть сучасні протоколи захисту можуть мати певні вразливості, які використовуються зловмисниками для проведення атак на бездротові мережі.

Однією з найвідоміших є атака на протокол WEP. Через недоліки алгоритму шифрування цей протокол вважається застарілим та небезпечним. Зловмисник може перехопити достатню кількість мережевих пакетів та за допомогою спеціального програмного забезпечення визначити пароль мережі. Саме через це використання WEP сьогодні не рекомендується.

Протокол WPA був створений для усунення недоліків WEP, проте і він має певні вразливості. Одним із поширених методів атаки є перехоплення процедури підключення користувача до мережі, яка називається handshake. Після отримання цих даних зловмисник може виконувати підбір пароля за допомогою

словникових атак або спеціальних програм для автоматичного перебору паролів. Якщо пароль є слабким або коротким, його можна відносно швидко визначити.

WPA2 тривалий час вважався найбільш надійним стандартом захисту бездротових мереж. Однак з розвитком методів атак були виявлені певні вразливості і в цьому протоколі. Однією з найбільш відомих є атака KRACK, яка дозволяє повторно використовувати ключі шифрування під час передачі даних. Це може дати змогу зловмиснику перехоплювати або змінювати інформацію, що передається мережею [9].

Ще однією поширеною атакою є підбір пароля до Wi-Fi мережі. Для цього використовуються словники найбільш популярних паролів або метод повного перебору комбінацій. Якщо користувач використовує простий пароль, наприклад дату народження або коротке слово, імовірність успішного злому значно зростає. Саме тому рекомендується використовувати складні паролі, які містять літери різного регістру, цифри та спеціальні символи.

Також небезпеку становлять атаки із створенням підроблених точок доступу. У такому випадку зловмисник створює Wi-Fi мережу зі схожою назвою, до якої можуть підключатися користувачі. Після підключення атакуючий отримує можливість перехоплювати дані або змінювати мережевий трафік. Опис атак та їхні наслідки можна подивитися у табл. 2.1.

Таблиця 2.1– Основні атаки на протоколи шифрування

Тип атаки	Опис атаки	Можливі наслідки
Атака на WEP	Перехоплення пакетів даних та визначення ключа шифрування	Отримання пароля та доступу до мережі
Словникова атака	Підбір пароля за допомогою словника популярних комбінацій	Несанкціонований доступ до Wi-Fi мережі
Brute Force атака	Повний перебір можливих варіантів пароля	Злам слабкого пароля
KRACK-атака	Повторне використання ключів шифрування WPA2	Перехоплення або зміна даних

Сучасний протокол WPA3 має значно кращий рівень захисту порівняно з попередніми версіями. У ньому використовуються вдосконалені механізми автентифікації та захисту від підбору паролів.

Проте навіть WPA3 не гарантує абсолютної безпеки, оскільки рівень захисту мережі також залежить від правильного налаштування обладнання та дотримання правил кібербезпеки користувачами.

Таким чином, атаки на протоколи шифрування є серйозною загрозою для бездротових мереж. Використання сучасних стандартів захисту, складних паролів та регулярне оновлення мережевого обладнання дозволяє значно зменшити ризик несанкціонованого доступу та витоку інформації [9].

Атака PMKID є ще одним сучасним методом злому мереж WPA2. На відміну від класичного перехоплення handshake, ця атака не вимагає присутності реального клієнта в мережі. Зловмисник надсилає один запит до точки доступу та отримує ідентифікатор ключа (PMKID), що містить достатньо інформації для подальшого підбору пароля в автономному режимі. Завдяки цьому атака є більш ефективною і менш помітною порівняно з традиційними методами.

Атаки типу Deauthentication (деавтентифікація) дозволяють зловмиснику примусово відключати користувачів від мережі шляхом надсилання підроблених пакетів деасоціації від імені точки доступу. Це використовується для перехоплення handshake при повторному підключенні клієнта або для організації атак типу відмови в обслуговуванні. Стандарт WPA3 частково вирішує цю проблему завдяки механізму Protected Management Frames (PMF), який захищає керуючі кадри від підробки. Порівняння методів атак на протоколи шифрування відображено в таблиці 2.2.

Таблиця 2.2 – Порівняння методів атак на протоколи шифрування

Тип атаки	Цільовий протокол	Складність	Засоби захисту
WEP cracking	WEP	Низька	Перехід на WPA2/WPA3
Handshake capture + брутфорс	WPA/WPA2	Середня	Складний пароль (16+ символів)
PMKID атака	WPA2	Середня	Перехід на WPA3 (SAE)
KRACK	WPA2	Висока	Оновлення прошивки, WPA3
Deauthentication	WPA/WPA2/WPA3	Низька	Увімкнення PMF (Protected Management Frames)

2.3 Перехоплення трафіку та атаки типу «Man-in-the-Middle» (MITM)

Одними з найбільш небезпечних загроз у бездротових мережах є перехоплення трафіку та атаки типу «людина посередині» (Man-in-the-Middle, MITM). Їхня особливість полягає в тому, що вони можуть відбуватися приховано для користувача і при цьому дозволяють зловмиснику отримувати доступ до великого обсягу конфіденційної інформації. У сучасних умовах, коли більшість даних передається через Інтернет, такі атаки становлять серйозну проблему для кібербезпеки [9].

Перехоплення трафіку (packet sniffing) базується на тому, що дані в бездротовій мережі передаються у вигляді радіосигналу. Це означає, що будь-який пристрій у зоні дії мережі може «слухати» ефір і фіксувати пакети даних, які передаються між користувачем і точкою доступу. У випадку недостатнього захисту або використання застарілих методів шифрування частина інформації може бути доступною для аналізу у відносно зрозумілому вигляді. Навіть якщо дані зашифровані, сам факт аналізу трафіку дозволяє отримати корисну інформацію: які сервіси використовуються, коли саме відбувається активність, які пристрої підключені до мережі.

Більш складним варіантом атаки є MITM, тобто ситуація, коли зловмисник не просто спостерігає за трафіком, а активно втручається в процес передачі даних. У такому випадку він стає «посередником» між користувачем і сервером або роутером. Для обох сторін виглядає так, ніби вони напряму взаємодіють, але

насправді весь трафік проходить через сторонній пристрій. Це дозволяє не тільки перехоплювати інформацію, а й змінювати її в реальному часі.

У бездротових мережах MITM-атаки можуть реалізовуватися різними способами. Один із найпоширеніших варіантів – створення підробленої точки доступу з назвою, схожою або ідентичною до легітимної мережі. Користувач підключається до такої мережі, вважаючи її справжньою, після чого весь його трафік проходить через пристрій зловмисника. Інший варіант – це перехоплення процесу з'єднання між пристроєм і роутером із подальшою підміною або перенаправленням даних.

Також існують сценарії, коли атакуючий впливає на таблиці маршрутизації або використовує підміну MAC-адрес у локальній мережі. У результаті пристрої починають передавати дані не на справжній шлюз, а на пристрій зловмисника.

Найбільшу небезпеку подібні атаки становлять у публічних Wi-Fi мережах. У кафе, готелях, торгових центрах або аеропортах користувачі часто підключаються до мережі без перевірки її справжності. У таких умовах зловмиснику досить просто створити фальшиву точку доступу з привабливою назвою, щоб отримати доступ до великої кількості користувачів одночасно. На рисунку 2.1 відображено, як працюють ці атаки.

Рисунок 2.1 – Атаки типу «людина посередині»

Для захисту від MITM-атак у бездротових мережах застосовуються різні технічні заходи. Одним із найефективніших є використання протоколу HTTPS для всіх веб-з'єднань. Наявність сертифіката TLS дозволяє переконатися, що користувач взаємодіє із справжнім сервером, а не з підробленим ресурсом зловмисника. Більшість сучасних браузерів автоматично попереджають користувача у разі підозрілого сертифіката або його відсутності.

Ефективним засобом захисту від перехоплення трафіку є використання VPN (Virtual Private Network). VPN-з'єднання шифрує весь мережевий трафік між пристроєм користувача та VPN-сервером, що унеможливлює перехоплення та аналіз переданих даних. Особливо важливо використовувати VPN під час підключення до публічних бездротових мереж, де ризик атак є найвищим.

Додатковим заходом захисту слугує технологія Dynamic ARP Inspection (DAI), яка застосовується в корпоративних мережах. Вона дозволяє перевіряти легітимність ARP-пакетів та запобігати підміні IP-адрес у локальній мережі. У поєднанні з функцією DHCP Snooping ці технології створюють надійний захист від ARP-спуфінгу, який є поширеним способом реалізації MITM-атак у бездротових мережах. Основні характеристики MITM-атак та відповідні заходи захисту систематизовано у таблиці 2.3.

Таблиця 2.3 – Характеристика MITM-атак та засоби захисту

Варіант MITM-атаки	Механізм реалізації	Засоби захисту
Evil Twin (підроблена AP)	Створення точки доступу з ідентичним SSID	VPN, перевірка сертифікатів
ARP Spoofing	Підміна MAC-адреси шлюзу в ARP-таблиці	Dynamic ARP Inspection, DHCP Snooping
SSL Stripping	Примусовий перехід від HTTPS до HTTP	HSTS, перевірка адресного рядка браузера
DNS Spoofing	Підміна DNS-відповідей для перенаправлення	DNSSEC, VPN, DoH (DNS over HTTPS)

2.4 Несанкціонований доступ і підбір паролів

Несанкціонований доступ до бездротових мереж є однією з найбільш актуальних проблем у сфері кібербезпеки. Через широке використання Wi-Fi у домашніх, навчальних та корпоративних мережах зловмисники постійно

шукають способи отримання доступу до мережевого обладнання та інформаційних ресурсів. Основною причиною успішних атак часто стає недостатній рівень захисту мережі, використання слабких паролів або неправильне налаштування маршрутизатора.

Бездротові мережі передають інформацію за допомогою радіосигналу, який може бути перехоплений будь-яким пристроєм у зоні покриття. Саме тому бездротові технології більш вразливі до несанкціонованого доступу порівняно з дротовими мережами. Якщо мережа захищена ненадійним паролем або застарілим протоколом шифрування, зловмисник може отримати доступ до неї за допомогою спеціального програмного забезпечення.

Одним із найпоширеніших способів злому є підбір пароля. У багатьох випадках користувачі використовують прості комбінації символів, які легко вгадати або автоматично підібрати. Часто для створення паролів застосовуються дати народження, номери телефонів, імена або стандартні слова. Подібні паролі не забезпечують належного рівня захисту, оскільки сучасні програми для злому можуть перевіряти тисячі або навіть мільйони варіантів за короткий проміжок часу.

Підбір паролів може здійснюватися декількома методами. Найпростішим є словникова атака, під час якої використовуються готові бази популярних паролів і слів. Якщо пароль складається зі звичайного слова або простої комбінації символів, ймовірність його успішного злому значно зростає. Іншим методом є brute force-атака, яка полягає у повному переборі всіх можливих комбінацій символів. Такий спосіб потребує більше часу, проте він є ефективним проти коротких і простих паролів.

Ще одним поширеним способом отримання доступу є використання стандартних налаштувань маршрутизатора. Багато користувачів після встановлення роутера не змінюють заводський логін і пароль адміністратора. Інформація про стандартні облікові дані часто знаходиться у відкритому доступі в мережі Інтернет або в інструкції до пристрою. У результаті зловмисник може

отримати повний контроль над мережевим обладнанням, змінити налаштування безпеки, переглядати трафік або заблокувати доступ законним користувачам.

Небезпеку також становлять атаки із перехопленням handshake-пакетів. Під час підключення користувача до Wi-Fi мережі між пристроєм та маршрутизатором відбувається процес автентифікації. Зловмисник може перехопити цей обмін даними та використовувати його для подальшого підбору пароля в автономному режимі. Такий метод часто застосовується проти мереж із протоколом WPA або WPA2.

Окрему загрозу створюють фальшиві точки доступу. У цьому випадку зловмисник створює бездротову мережу з назвою, схожою на справжню. Користувачі можуть помилково підключитися до такої мережі, після чого їхні дані передаватимуться через пристрій атакуючого. Це дозволяє перехоплювати паролі, особисту інформацію та інші конфіденційні дані. Розглянути характеристику атак та наслідки можна у таблиці 2.4.

Таблиця 2.4 – Характеристика атак

Спосіб атаки	Характеристика	Можливі наслідки
Brute Force-атака	Повний автоматичний перебір паролів	Отримання доступу до Wi-Fi мережі
Словникова атака	Використання баз популярних слів і комбінацій	Злам слабких паролів
Використання стандартних облікових даних	Застосування заводських логінів і паролів	Захоплення контролю над роутером
Перехоплення handshake	Захоплення процесу автентифікації користувача	Подальший підбір ключа безпеки
Фальшива точка доступу	Створення підробленої Wi-Fi мережі	Викрадення конфіденційної інформації
Соціальна інженерія	Отримання пароля шляхом обману користувача	Несанкціонований доступ до мережі

У сучасних умовах атаки на бездротові мережі стають дедалі складнішими та автоматизованими. Для злому можуть використовуватися спеціальні програми аналізу трафіку та тестування безпеки мереж. Такі інструменти дозволяють виявляти тип шифрування, аналізувати пакети даних та проводити

атаки на автентифікацію користувачів. Особливо небезпечними є ситуації, коли користувачі нехтують базовими правилами кібербезпеки.

Для захисту бездротової мережі необхідно використовувати складні та унікальні паролі, які містять великі й малі літери, цифри та спеціальні символи. Довжина пароля також має велике значення, оскільки довші комбінації значно ускладнюють процес підбору. Не рекомендується використовувати особисту інформацію або прості слова, які легко вгадати.

Крім цього, важливо застосовувати сучасні протоколи шифрування, зокрема WPA2 або WPA3. Застарілі стандарти, такі як WEP, мають серйозні вразливості та можуть бути зламані за короткий час. Також необхідно регулярно оновлювати програмне забезпечення маршрутизатора, оскільки виробники часто виправляють знайдені помилки безпеки у нових версіях прошивки.

Додатковими заходами захисту є вимкнення функції WPS, зміна стандартної назви мережі, фільтрація MAC-адрес та контроль списку підключених пристроїв. Регулярний моніторинг мережі дозволяє своєчасно виявляти підозрілу активність та запобігати можливим атакам [4; 8].

РОЗДІЛ 3 МЕТОДИ ДОСЛІДЖЕННЯ ТА ПІДВИЩЕННЯ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ

3.1 Інструменти аналізу та моніторингу бездротових мереж

Сучасні бездротові мережі широко використовуються у різних сферах діяльності: у домашньому користуванні, офісах, навчальних закладах, державних установах, промисловості та на підприємствах. Завдяки своїй мобільності, простоті підключення та високій швидкості передачі даних бездротові технології стали невід'ємною частиною інформаційної інфраструктури. Однак разом із перевагами виникають і серйозні загрози безпеці, оскільки передача даних здійснюється через радіоканал, який може бути доступним для сторонніх осіб. Саме тому важливе значення мають інструменти аналізу та моніторингу бездротових мереж, які дозволяють контролювати стан мережі, виявляти вразливості та своєчасно реагувати на потенційні загрози.

Моніторинг бездротової мережі – це процес постійного спостереження за роботою мережевого обладнання, передачею трафіку, рівнем сигналу, кількістю підключених пристроїв та іншими параметрами функціонування мережі. Основною метою моніторингу є забезпечення стабільної роботи мережі та виявлення підозрілої активності. Аналіз бездротової мережі дозволяє оцінити рівень захищеності мережі, визначити наявні недоліки та перевірити ефективність застосованих засобів захисту.

Одним із найважливіших інструментів аналізу мережевого трафіку є Wireshark. Це програмне забезпечення використовується для перехоплення та детального аналізу пакетів даних, які передаються через мережу. За допомогою Wireshark можна переглядати структуру пакетів, визначати джерело та призначення трафіку, аналізувати протоколи передачі даних і виявляти підозрілу активність. Програма підтримує велику кількість мережевих протоколів і дозволяє отримувати повну інформацію про роботу мережі в режимі реального часу [7].

Ще одним популярним засобом аналізу бездротових мереж є Kismet. Цей інструмент призначений для виявлення бездротових мереж, прихованих точок доступу та підключених клієнтів. Kismet працює у пасивному режимі, тобто не взаємодіє безпосередньо з мережею, а лише прослуховує радіоефір. Завдяки цьому зменшується ризик виявлення самого процесу моніторингу. Програма дозволяє визначати тип шифрування, рівень сигналу та характеристики бездротових мереж, що є важливим під час проведення аудиту безпеки.

Для перевірки надійності захисту Wi-Fi мереж часто використовується набір інструментів Aircrack-ng. Цей програмний комплекс призначений для аналізу бездротових мереж, перехоплення пакетів та тестування стійкості паролів. За допомогою Aircrack-ng можна оцінити рівень захищеності мереж WPA, WPA2 та WEP, а також виявити слабкі місця у конфігурації мережевого обладнання. Інструмент широко використовується спеціалістами з кібербезпеки для проведення тестування на проникнення та перевірки ефективності засобів захисту.

Важливу роль у моніторингу бездротових мереж відіграють також системи централізованого управління мережею. Вони дозволяють адміністраторам отримувати інформацію про стан мережевого обладнання, навантаження на точки доступу, рівень сигналу та можливі збої в роботі мережі. Такі системи автоматично формують звіти, попереджають про підозрілу активність та допомагають швидко реагувати на інциденти безпеки [10].

Для аналізу параметрів бездротової мережі використовуються також спеціальні мобільні додатки та утиліти. Наприклад, програми для аналізу Wi-Fi сигналу дозволяють визначати рівень покриття мережі, перевіряти зайнятість каналів та знаходити оптимальне місце для встановлення точки доступу. Це допомагає зменшити рівень перешкод та підвищити стабільність роботи мережі.

Окрему увагу слід приділити системам виявлення вторгнень у бездротових мережах. Такі системи аналізують мережевий трафік і автоматично визначають підозрілі дії користувачів або спроби атак. Наприклад, вони можуть виявляти спроби підбору паролів, створення фальшивих точок доступу або аномальну

активність у мережі. У разі виявлення загрози система повідомляє адміністратора або автоматично блокує небезпечне підключення [11]. Розглянути переваги та недоліки можна у таблиці 3.1.

Таблиця 3.1 – Переваги та недоліки інструментів

Інструмент	Переваги	Недоліки	Сфера застосування
Wireshark	Детальний аналіз трафіку, зручний інтерфейс	Потребує додаткових засобів для аудиту Wi-Fi	Аналіз мережевого трафіку
Kismet	Пасивний моніторинг, виявлення прихованих мереж	Складніше налаштування	Моніторинг бездротових мереж
Aircrack-ng	Широкі можливості тестування Wi-Fi	Потребує спеціальних навичок	Тестування захищеності мереж

За результатами проведеного порівняльного аналізу встановлено, що кожен із розглянутих інструментів має власну спеціалізацію у сфері моніторингу та аналізу бездротових мереж. Wireshark є найбільш ефективним для детального аналізу мережевого трафіку та діагностики мережевих процесів [7]. Kismet доцільно використовувати для пасивного моніторингу бездротового середовища та виявлення прихованих точок доступу. Aircrack-ng застосовується для перевірки надійності захисту Wi-Fi мереж та оцінювання їх рівня безпеки [8]. Таким чином, найкращі результати досягаються при комплексному використанні даних інструментів залежно від поставлених завдань.

3.2 Проведення тестування захищеності мережі

Практична частина цієї роботи присвячена перевірці захищеності бездротової мережі офісу. Для цього ми провели тестування на проникнення – тобто змоделювали дії хакера, щоб знайти слабкі місця в налаштуваннях Wi-Fi ще до того, як ними скористаються реальні зловмисники.

Для створення мережі та аналізу трафіка ми використали програму Cisco Packet Tracer. Вона дозволяє побудувати точну схему мережі, налаштувати роутер та покроково відстежити, як саме летять пакети даних між пристроями.

Тестування проводилося за умови, що хакер (Attacker_Laptop) спочатку не знає паролів і не має доступу до роутера, а просто знаходиться в радіусі дії Wi-Fi сигналу. Щоб показати різницю в рівнях безпеки, потрібно розбити дослідження на два окремі варіанти.

У першому варіанті було досліджено рівень безпеки мережі, захищеної лише стандартним протоколом шифрування WPA2-Personal, за умови відсутності додаткових засобів контролю доступу клієнтів.

Під час симуляції було змодельовано ситуацію, коли умовний зловмисник (Attacker_Laptop) успішно скомпрометував спільний ключ доступу (наприклад, через словникову атаку або використання простих парольних комбінацій). За наявності коректного пароля пристрій зловмиснику безперешкодно проходить етапи автентифікації та асоціації з точкою доступу WRT300N.

У режимі покрокової симуляції трафіка чітко зафіксовано, що маршрутизатор починає обслуговувати пристрій хакера на рівні з легітимними користувачами, спрямовуючи маркери бездротового трафіка (пакети даних) у його бік.

Даний експеримент доводить, що використання лише парольного захисту є недостатнім для забезпечення надійного безпекового периметра. У разі компрометації ключа зловмисник отримує повний доступ до внутрішнього сегменту мережі, що дозволяє йому здійснювати деструктивний вплив: сканувати робочі станції, перехоплювати транзитні пакети та реалізовувати атаки класу MITM (Man-In-The-Middle). Побачити приклад незахищеної мережі можна на рисунку 3.1.

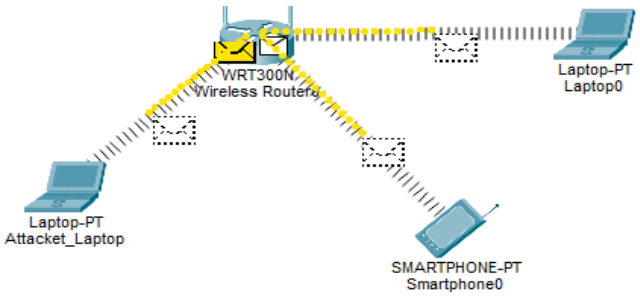

Рисунок 3.1 – Зразок незахищеної мережі

У другому варіанті конфігурацію безпеки досліджуваної мережі було посилено за допомогою фільтрації Mac-адрес.

Для цього в налаштуваннях маршрутизатора було активовано функцію Wireless MAC Filter у режимі Permit only (Дозволити лише переліченим). До апаратної бази даних пристрою було внесено виключно унікальні 12-значні фізичні адреси легітимного ноутбука (Laptop0) та смартфона (Smartphone0), записані у вигляді суцільного шістнадцяткового рядка без розділових знаків для коректної обробки довжини кадру.

В результаті повторного моделювання можна помітити високу ефективність впровадженого заходу:

– Маршрутизатор миттєво розірвав бездротову сесію з пристроєм Attacker_Laptop та скасував його асоціацію.

– У режимі симуляції пакети даних циркулюють виключно між точкою доступу та авторизованими пристроями працівників.

– Будь-які спроби повторного підключення або відправки кадрів з боку неавторизованого ноутбука автоматично блокуються та відкидаються маршрутизатором на етапі радіообміну.

Приклад захищеної мережі шляхом фільтрації Mac-адрес можна на рисунках 3.2 та 3.3.

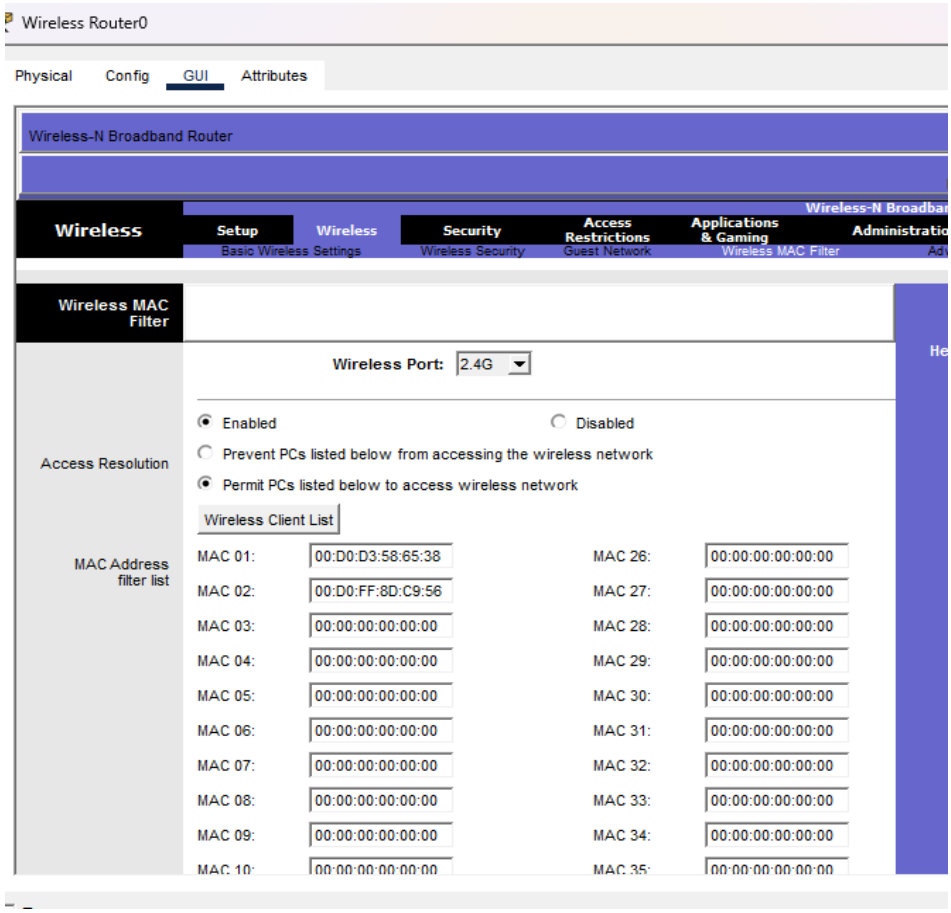

Рисунок 3.2 – Фільтрація Mac-адрес

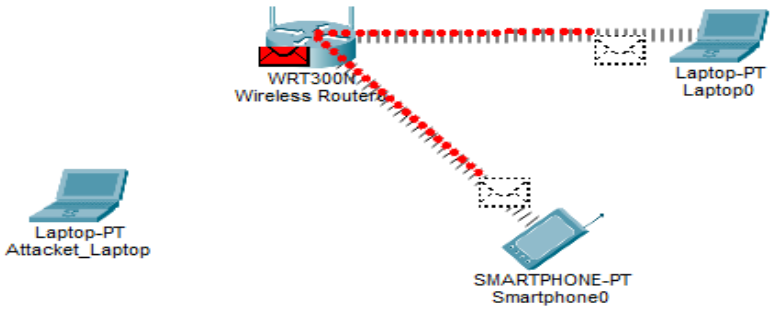

Рисунок 3.3 – Зразок захищеної мережі

Активація білих списків створює додатковий стійкий рубіж оборони. Оскільки унікальної апаратної адреси зловмисника немає в переліку довірених, точка доступу ігнорує його запити на апаратному рівні. Це повністю скасовує загрозу несанкціонованого проникнення в мережу, навіть якщо основний ключ

WPA2 було попередньо скомпрометовано. Порівняння двох варіантів наочно довело, що використання лише одного пароля (WPA2-Personal) є критично вразливим: у разі його компрометації хакер легко потрапляє у внутрішню мережу, отримує можливість сканувати робочі станції та перехоплювати пакети (атаки MITM).

Впровадження другого рубежу захисту у вигляді фільтрації MAC-адрес повністю нейтралізувало цю загрозу. Навіть знаючи правильний пароль, пристрій зловмисника був миттєво заблокований роутером на етапі радіообміну через відсутність його адреси у «білому списку». Це дозволило надійно ізолювати хакера та захистити конфіденційність внутрішнього трафіка офісу.

3.3 Оцінка ризиків та аналіз безпеки бездротових мереж

Після проведення тестування бездротової мережі та моделювання можливих сценаріїв атак виникає необхідність оцінити рівень ризиків, пов’язаних з її експлуатацією. Оцінка ризиків є важливим етапом забезпечення інформаційної безпеки, оскільки дозволяє визначити найбільш небезпечні загрози, оцінити можливі наслідки їх реалізації та обґрунтувати необхідність впровадження додаткових заходів захисту.

Особливістю бездротових мереж є використання радіоканалу для передавання даних. На відміну від дротових мереж, фізичний доступ до кабельної інфраструктури не є обов’язковим для здійснення атаки. Будь-який користувач, який перебуває в зоні покриття сигналу, потенційно може спробувати отримати доступ до мережі або здійснити аналіз передаваного трафіку. Саме тому бездротові мережі потребують більш ретельного підходу до організації захисту.

На основі проведеного дослідження було визначено основні загрози, характерні для бездротових мереж. Найбільш небезпечним ризиком є несанкціонований доступ до мережі внаслідок компрометації пароля бездротового з’єднання. У разі успішного отримання облікових даних сторонній користувач фактично стає повноправним учасником локальної мережі та

отримує можливість взаємодіяти з іншими пристроями. Наслідком такої ситуації може бути отримання доступу до внутрішніх ресурсів, збір інформації про мережеву інфраструктуру, а також підготовка до реалізації більш складних атак.

Значний рівень небезпеки також становить ризик перехоплення мережевого трафіку. Після отримання доступу до мережі зловмисник може аналізувати передані дані та збирати інформацію про мережеву активність користувачів. Особливо небезпечними є випадки використання незахищених сервісів або неправильного налаштування мережевого обладнання. У таких умовах існує ймовірність розкриття конфіденційної інформації або облікових даних користувачів.

Окрему категорію становлять атаки типу «людина посередині» (Man-in-the-Middle). Під час таких атак зловмисник отримує можливість втручатися у процес обміну даними між двома вузлами мережі. Наслідками можуть бути модифікація переданої інформації, перенаправлення користувачів на сторонні ресурси або викрадення конфіденційних даних. Хоча реалізація подібних атак потребує додаткових дій з боку зловмисника, їх потенційний вплив на безпеку мережі є досить значним.

Під час аналізу було встановлено, що ризик реалізації атак значною мірою залежить від налаштувань мережевого обладнання та застосованих механізмів захисту. Зокрема, використання лише пароля доступу до бездротової мережі не забезпечує достатнього рівня безпеки у випадку його розголошення або успішного підбору. З цієї причини доцільно використовувати додаткові засоби контролю доступу, які дозволяють обмежити коло пристроїв, що можуть підключатися до мережі.

Одним із таких механізмів є фільтрація MAC-адрес. Аналіз результатів моделювання показав, що застосування MAC-фільтрації дозволяє знизити ймовірність несанкціонованого підключення до мережі навіть у випадку компрометації пароля. Однак даний механізм не може розглядатися як самостійний засіб захисту, оскільки існують способи підроблення MAC-адрес.

Тому його використання є доцільним лише у поєднанні з іншими методами захисту.

Для більш наочного представлення результатів аналізу ризики було класифіковано за рівнем їх впливу на безпеку мережі. До категорії високих ризиків віднесено несанкціонований доступ до мережі, компрометацію облікових даних та перехоплення трафіку. Середній рівень ризику мають атаки типу «людина посередині» та спроби обходу механізмів контролю доступу. Низький рівень ризику характерний для загроз, реалізація яких потребує спеціалізованого обладнання або значних технічних знань.

Проведена оцінка показала, що найбільшу небезпеку для бездротової мережі становлять загрози, пов’язані з отриманням доступу до мережевої інфраструктури сторонніми особами. Саме тому основна увага під час побудови системи захисту повинна приділятися забезпеченню надійної автентифікації користувачів, використанню сучасних протоколів шифрування та впровадженню додаткових механізмів контролю доступу.

Таким чином, проведений аналіз дозволив визначити основні ризики, характерні для бездротових мереж, та оцінити їх можливий вплив на інформаційну безпеку. Отримані результати підтверджують необхідність комплексного підходу до захисту бездротової мережі, який передбачає поєднання організаційних і технічних заходів безпеки. Результати оцінки ризиків можуть бути використані для розроблення рекомендацій щодо підвищення рівня захисту бездротових мереж, які розглядаються в наступному підрозділі.

Для систематизації виявлених загроз було застосовано матрицю ризиків, яка дозволяє оцінити кожну загрозу за двома параметрами: ймовірністю її реалізації та потенційним впливом на інформаційну безпеку організації. Такий підхід є стандартним у сфері управління ризиками інформаційної безпеки та відповідає вимогам стандарту ISO/IEC 27005 [12]. Матрицю ризиків для досліджуваної бездротової мережі наведено у таблиці 3.2.

Таблиця 3.2 – Матриця ризиків інформаційної безпеки бездротової мережі

Загроза	Ймовірність	Вплив	Рівень ризику	Пріоритет
Несанкціонований доступ (злам пароля)	Висока	Критичний	Критичний	1
Перехоплення трафіку	Середня	Високий	Високий	2
MITM-атака	Середня	Критичний	Високий	3
DoS/DDoS-атака	Низька	Середній	Середній	4
Підроблена точка доступу	Висока	Високий	Критичний	1
Витік через застаріле ПЗ роутера	Середня	Середній	Середній	3

Аналіз матриці ризиків свідчить, що найбільш критичними загрозами для бездротової мережі є несанкціонований доступ внаслідок злому пароля та підключення до підробленої точки доступу. Обидві загрози мають високу ймовірність реалізації та значний потенційний вплив на конфіденційність і цілісність інформації. Саме тому першочергова увага при розробці системи захисту повинна приділятися саме цим ризикам.

Перехоплення трафіку та MITM-атаки класифіковано як загрози з високим рівнем ризику. Хоча їх ймовірність дещо нижча порівняно з першою групою, потенційний вплив залишається значним через можливість отримання конфіденційних даних у реальному часі. Загрози, пов’язані з DoS-атаками та застарілим програмним забезпеченням роутера, мають середній рівень ризику та можуть бути мінімізовані шляхом регулярного оновлення обладнання та налаштування засобів захисту від атак на доступність.

3.4 Рекомендації щодо підвищення рівня захисту бездротових мереж

Проведений аналіз безпеки бездротової мережі та результати моделювання можливих сценаріїв атак показали, що основними загрозами є несанкціонований доступ до мережі, перехоплення трафіку та отримання доступу до внутрішніх ресурсів після компрометації пароля. З огляду на виявлені ризики було сформовано комплекс рекомендацій, спрямованих на підвищення рівня захищеності бездротової мережі.

Насамперед доцільно використовувати сучасні протоколи шифрування бездротового з’єднання. У процесі дослідження було встановлено, що отримання пароля від мережі фактично надає зловмиснику доступ до внутрішнього сегмента мережі. Для зменшення ймовірності реалізації таких атак рекомендується використовувати протокол WPA3, який забезпечує вищий рівень захисту порівняно з попередніми стандартами. Якщо обладнання не підтримує WPA3, слід застосовувати WPA2 із шифруванням AES та відмовитися від використання застарілих протоколів WEP і WPA [6].

Важливим заходом захисту є підвищення вимог до паролів бездротової мережі. Пароль повинен мати достатню довжину та складність, щоб ускладнити його підбір за допомогою автоматизованих засобів. Рекомендується використовувати комбінації великих і малих літер, цифр та спеціальних символів. Крім того, доцільно періодично змінювати пароль і не використовувати типові або легко передбачувані комбінації.

У результаті проведеного моделювання встановлено, що додатковим механізмом захисту може бути фільтрація MAC-адрес. Після впровадження цього механізму доступ до мережі отримували лише пристрої, які були попередньо внесені до списку дозволених. Незважаючи на те, що MAC-фільтрація не гарантує абсолютного захисту від досвідченого зловмисника, вона створює додатковий рівень контролю доступу та ускладнює реалізацію несанкціонованих підключень.

Окрему увагу необхідно приділити налаштуванню мережевого обладнання. Після встановлення маршрутизатора рекомендується змінити стандартні облікові дані адміністратора, оскільки заводські логіни та паролі часто є загальновідомими.

Важливим елементом захисту є своєчасне оновлення програмного забезпечення маршрутизатора. Виробники мережевого обладнання регулярно випускають оновлення, які усувають виявлені вразливості та покращують механізми захисту.

Для своєчасного виявлення можливих інцидентів рекомендується здійснювати моніторинг підключених пристроїв та аналіз журналів подій маршрутизатора. Регулярна перевірка списку активних підключень дозволяє виявити невідомі пристрої та оперативно реагувати на спроби несанкціонованого доступу до мережі. Для узагальнення запропонованих рекомендацій складено таблиці 3.3.

Таблиця 3.3 – Рекомендації щодо підвищення рівня захисту бездротових мереж

Загроза	Можливі наслідки	Рекомендовані заходи захисту
Підбір пароля Wi-Fi	Несанкціонований доступ до мережі	Використання складних паролів та їх регулярна зміна
Перехоплення трафіку	Витік конфіденційної інформації	Шифрування даних та використання захищених протоколів
MITM-атаки	Викрадення або модифікація інформації	Контроль мережевих підключень та використання сучасних засобів захисту
Підключення сторонніх пристроїв	Порушення цілісності та конфіденційності даних	Фільтрація MAC-адрес та моніторинг мережі
Використання застарілого ПЗ	Експлуатація відомих вразливостей	Регулярне оновлення прошивки обладнання
Людський фактор	Помилки користувачів та витік інформації	Навчання користувачів правилам кібербезпеки

Таким чином, підвищення рівня захисту бездротових мереж можливе лише за умови комплексного застосування різних механізмів безпеки. Поєднання сучасних протоколів шифрування, надійної автентифікації, контролю доступу, регулярного оновлення обладнання та постійного моніторингу мережі дозволяє значно зменшити ризик реалізації найбільш поширених загроз.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи на тему «Захист бездротових мереж та дослідження їх вразливостей» було розглянуто особливості роботи бездротових мереж, сучасні методи їх захисту та основні загрози, які можуть виникати під час використання бездротового зв’язку. Сьогодні бездротові мережі використовуються майже всюди – вдома, у навчальних закладах, офісах, державних установах та громадських місцях, тому питання їх безпеки є дуже актуальним.

У першому розділі було досліджено основні принципи роботи бездротових мереж та їх класифікацію. Також були розглянуті популярні стандарти бездротового зв’язку, зокрема Wi-Fi, Bluetooth, LTE та 5G, їхні особливості, переваги та сфери застосування. Окрему увагу приділено протоколам шифрування WEP, WPA, WPA2 та WPA3. Під час аналізу було встановлено, що старі стандарти захисту вже не можуть забезпечити належний рівень безпеки, оскільки мають значну кількість вразливостей. Натомість сучасні технології шифрування дозволяють значно краще захищати передані дані від перехоплення та несанкціонованого доступу. Також було розглянуто методи автентифікації користувачів і засоби контролю доступу, які допомагають обмежити підключення сторонніх пристроїв до мережі.

У другому розділі було проведено аналіз основних загроз і вразливостей бездротових мереж. У ході дослідження було визначено, що найбільшу небезпеку становлять атаки на протоколи шифрування, перехоплення мережевого трафіку, атаки типу «людина посередині» (MITM), а також підбір паролів. Крім технічних атак, значну роль відіграє і людський фактор. Багато проблем виникає через використання слабких паролів, неправильне налаштування мережі або недостатню обізнаність користувачів у сфері кібербезпеки. Також було розглянуто методи соціальної інженерії та фішингові атаки, за допомогою яких зловмисники можуть отримувати доступ до конфіденційної інформації шляхом введення користувачів в оману.

У третьому розділі були досліджені сучасні методи аналізу та підвищення безпеки бездротових мереж. Було розглянуто інструменти моніторингу та тестування мереж, які дозволяють виявляти вразливості та оцінювати рівень захищеності системи. У результаті дослідження було встановлено, що для ефективного захисту бездротової мережі необхідно використовувати комплексний підхід. До основних рекомендацій можна віднести використання сучасних стандартів шифрування, створення складних паролів, регулярне оновлення програмного забезпечення, обмеження доступу до мережі та постійний контроль мережевої активності. Також важливим фактором є підвищення рівня обізнаності користувачів щодо правил безпечної роботи в мережі.

Під час виконання роботи було підтверджено, що бездротові мережі мають як значні переваги, так і певні ризики, пов’язані з безпекою передачі даних. Через відкритий характер передачі сигналу такі мережі є більш вразливими до атак порівняно з дротовими мережами. Саме тому питання захисту бездротового середовища потребує постійної уваги та вдосконалення методів безпеки відповідно до сучасних кіберзагроз.

Отже, поставлена мета кваліфікаційної роботи була досягнута, а всі поставлені завдання виконані. У ході роботи було отримано теоретичні та практичні результати, які дозволяють краще зрозуміти принципи захисту бездротових мереж і способи протидії сучасним загрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Мікітишин А. Г., Митник М. М. Комп'ютерні мережі. Книга 1 : навчальний посібник. Львів : Магнолія 2006, 2013. 256 с. URL: https://elartu.tntu.edu.ua/bitstream/123456789/16930/5/Mykytyshyn_A_G_Mytnyk_M_M_Kompjuterni_merezhi_Knyga_1.pdf (дата звернення: 20.05.2026).

2 Бурячок В. Л., Толубко В. Б., Хорошко В. О. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Київ : ДУТ, 2015. 288 с. URL: https://duikt.edu.ua/uploads/l_1868_58378127.pdf (дата звернення: 20.05.2026)

3 Scarfone K., Heger A. Guide to Securing Wi-Fi Networks. National Institute of Standards and Technology. Gaithersburg : NIST, 2024. URL: https://www.nist.gov (дата звернення: 20.05.2026).

4 Гнатюк С. О., Сидоренко В. М. Основи кібербезпеки та захисту інформації : навчальний посібник. Київ : НАУ, 2021. 304 с. URL: https://er.nau.edu.ua/handle/NAU/53054 (дата звернення: 20.05.2026).

5 IEEE Standards Association. 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. New York : IEEE, 2024. URL: https://standards.ieee.org/ieee/802.11 (дата звернення: 20.05.2026).

6 Cisco Systems. Wireless Security Best Practices. San Jose : Cisco Systems, 2025. URL: https://www.cisco.com/c/en/us/products/wireless/index.html (дата звернення: 20.05.2026).

7 Orebaugh A., Ramirez G., Burke E. Wireshark & Ethereal Network Protocol Analyzer Toolkit. Burlington : Syngress Publishing, 2007. 432 p. URL: https://www.elsevier.com/books/wireshark-and-ethereal-network-protocol-analyzer-toolkit/orebaugh/978-1-59749-073-3 (дата звернення: 20.05.2026).

8 Kali Linux Documentation. Wireless Attacks and Penetration Testing Guide. Offensive Security, 2025. URL: https://www.kali.org/docs (дата звернення: 20.05.2026).

9 Vanhoef M., Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. Proceedings of the ACM Conference on Computer and Communications Security. 2017. P. 1313–1328. URL: https://papers.mathyvanhoef.com/ccs2017.pdf (дата звернення: 20.05.2026).

10 Hofstede R., Čeleda P., Trammell B., Drago I., Sadre R., Sperotto A., Pras A. Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX. IEEE Communications Surveys & Tutorials. 2014. Vol. 16, No. 4. P. 2037–2064. URL: https://research.utwente.nl/files/6519118/tutorial.pdf (дата звернення: 20.05.2026).

11 Najafimehr M., Zarifzadeh S., Mostafavi S. DDoS Attacks and Machine-Learning-Based Detection Methods: A Survey and Taxonomy. Engineering Reports. 2023. Vol. 5, No. 12. Article ID e12697. URL: https://onlinelibrary.wiley.com/doi/pdfdirect/10.1002/eng2.12697 (дата звернення: 20.05.2026).

12 NIST. Cybersecurity Framework 2.0. National Institute of Standards and Technology. 2024. URL: https://www.nist.gov/cyberframework (дата звернення: 20.05.2026).

13 Безчасний М.С., Люта М.В. Безпека та захист бездротових мереж: загрози та методи протидії. Матеріали XVIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених за тематикою «Тенденції розвитку ІТ-технологій в Україні». 23-24 квітня 2026 р., Черкаси, Україна. Черкаси: Черкаський державний фаховий бізнес-коледж, 2026. С. 30-32.