

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка

до дипломного проекту (роботи)

магістра

(ступінь вищої освіти)

на тему СИСТЕМА ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ ІЗ ВИКОРИСТАННЯМ
БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

Виконав: студент 2 курсу, групи КНТ-513м
спеціальності _____

123 Комп'ютерна інженерія

(код і найменування спеціальності)

Освітня програма (спеціалізація)

Комп'ютерні системи та мережі

БРЮХОВ Б. Р.

(ПРИЗВИЩЕ та ініціали)

Керівник КИРИЧЕК Г.Г.

(ПРИЗВИЩЕ та ініціали)

Рецензент ЄФИМЕНКО М.В.

(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти магістерський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)
Освітня програма (спеціалізація) «Комп'ютерні системи та мережі»
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Зав. кафедри Кудерметов Р.К.

“ ” 2024 року

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

БРЮХОВА Богдана Руслановича

(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Система захисту бездротових мереж із використанням багатofакторної автентифікації

керівник проєкту (роботи) к. т. н., доцент, КИРИЧЕК Галина Григорівна

(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)

затверджені наказом вищого навчального закладу від “18” жовтня 2024 року № 149

2. Строк подання студентом проєкту (роботи) 10 грудня 2024 року

3. Вихідні дані до проєкту (роботи) Система захисту бездротових мереж із використанням багатofакторної автентифікації. Бездротові мережі. IEEE 802.11 та її експлуатаційні характеристики. Стандарти: IEEE 802.11n/ac/ax. Види атак на бездротові мережі.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз стандартів та особливостей роботи бездротових мереж. Аналіз безпеки та технологій захисту бездротових мереж. Впровадження системи захисту бездротових мереж. Аналіз ефективності впроваджених методів захисту.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-5	КИРИЧЕК Г. Г., доцент		
нормоконтроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання 05.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Огляд літературних джерел за темою роботи	10.10.2024 р.	
2	Аналіз стандартів та особливостей роботи бездротових мереж	25.10.2024 р.	
3	Аналіз безпеки та технологій захисту бездротових мереж	05.11.2024 р.	
4	Види атак на бездротові мережі	12.11.2024 р.	
5	Впровадження системи захисту бездротових мереж	18.11.2024 р.	
6	Аналіз ефективності впроваджених методів захисту	25.11.2024 р.	
7	Оформлення отриманих результатів у ПЗ	30.11.2024 р.	
8	Проходження нормоконтролю	05.12.2024 р.	
9	Оформлення додаткового матеріалу	10.12.2024 р.	

Студент Богдан БРЮХОВ
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник проєкту (роботи) Галина КИРИЧЕК
(підпис) (ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

ПЗ: 68 с., 21 рис., 8 табл., 22 джерел

WPA3, MFA, БЕЗДРОТОВІ МЕРЕЖІ, WI-FI, IEEE 802.11, МІМО, МОДЕЛЬ ЗАХИСТУ, RADIUS, DDOS, MITM, БРУТФОРС, ШИФРУВАННЯ, ОТР, СЕРВЕР АВТЕНТИФІКАЦІЇ, KRACK, OWE, ЗАХИСТ МЕРЕЖІ

Мета роботи – забезпечення безпеки бездротових мереж шляхом впровадження системи захисту, яка поєднує сучасні методи шифрування та багатофакторну автентифікацію.

Об'єкт дослідження – процес передачі даних у бездротових мережах та забезпечення їх захисту.

Предмет дослідження – методи шифрування, автентифікації та засоби захисту бездротових мереж від сучасних кіберзагроз.

У роботі проведено аналіз сучасних стандартів бездротових мереж, зокрема WEP, WPA, WPA2 та WPA3, оцінено їх вразливості й ефективність. Обґрунтовано вибір WPA3 як оптимального стандарту для захисту, враховуючи його стійкість до атак та криптографічну надійність. Досліджено методи багатофакторної автентифікації, їх переваги та недоліки, а також спроектовано модель системи захисту, що включає кілька рівнів перевірки користувачів.

Проведено моделювання та тестування впровадженої системи в реальних умовах із використанням сучасних програмних інструментів. Результати показали підвищення рівня безпеки мережі, зменшення кількості вразливостей та збереження продуктивності навіть за високих навантажень.

Результати роботи можуть бути використані для модернізації існуючих бездротових мереж підприємств, зокрема у сфері фінансів, медицини та державного управління.

ABSTRACT

Explanatory note to the master's work: 68 p, 21 figures, 8 tables, 22 sources

WPA3, MFA, WIRELESS NETWORKS, WI-FI, IEEE 802.11, MIMO, SECURITY MODEL, RADIUS, DDOS, MITM, BRUTE FORCE, ENCRYPTION, OTP, AUTHENTICATION SERVER, KRACK, OWE, NETWORK SECURITY

The purpose of the study is to ensure the security of wireless networks by developing a security system that combines modern encryption methods and multi-factor authentication.

The object of research is the process of data transmission in wireless networks and ensuring their protection.

Subject of research - methods of encryption, authentication and means of protecting wireless networks from modern cyber threats.

Software: Cisco Packet Tracer, Microsoft Visio 2016.

The paper analyzes modern wireless network standards, in particular WEP, WPA, WPA2, and WPA3, and evaluates their vulnerabilities and effectiveness. The choice of WPA3 as the optimal standard for protection is substantiated, taking into account its resistance to attacks and cryptographic reliability. The methods of multifactor authentication, their advantages and disadvantages are investigated, and a model of a security system that includes several levels of user verification is designed.

The implemented system was modeled and tested in real conditions using modern software tools. The results showed an increase in the level of network security, a reduction in the number of vulnerabilities, and the preservation of performance even under high loads.

The results of the work can be used to modernize existing wireless networks of enterprises, in particular in the field of finance, medicine and public administration.

ЗМІСТ

Вступ.....	7
1 Аналіз стандартів та особливостей роботи бездротових мереж	8
1.1 Поняття та використання технології бездротової мережі Wi-Fi.....	8
1.2 Класифікація бездротових мереж.....	10
1.3 Аналіз сучасних стандартів та технологій бездротових мереж	13
1.4 Опис моделі захисту бездротових мереж	18
1.5 Постановка завдань	21
2 Аналіз безпеки та технологій захисту бездротових мереж	22
2.1 Головні види атак на бездротові мережі.....	22
2.2 Методи забезпечення безпеки бездротових мереж	32
3 Впровадження системи захисту бездротових мереж	40
3.1 Впровадження шифрування даних	41
3.2 Реалізація механізмів багатфакторної автентифікації.....	43
4 Аналіз ефективності впроваджених методів захисту.....	52
4.1 Оцінка впровадження WPA3 у бездротових мережах	53
4.2 Оцінка впровадження MFA та порівняння з альтернативами.....	57
4.3 Результати впровадження WPA3 та MFA в комплексі	60
Висновки	64
Перелік джерел посилання	66

ВСТУП

В умовах сучасного розвитку технологій, бездротові мережі стали невід'ємною частиною інфраструктури більшості організацій та приватних осіб. Бездротові системи зв'язку дозволяють передавати дані без необхідності фізичних з'єднань, що значно розширює їх можливості та робить їх зручнішими для використання. Проте, з розширенням застосування бездротових мереж збільшується і кількість загроз та вразливостей, пов'язаних з кібербезпекою.

Основною проблемою є те, що бездротова мережа схильна до різного роду атак, зокрема, атак типу "man-in-the-middle", перехоплення даних, атак на віддалений доступ та інших видів вторгнень. Особливу увагу слід приділити захисту даних, що передаються через бездротові мережі, оскільки такі мережі часто використовуються для критично важливих систем, зокрема, у фінансових та медичних закладах, в державних установах та бізнес-структурах.

Одним з ефективних методів захисту є багатофакторна автентифікація (MFA), яка забезпечує додатковий рівень захисту шляхом підтвердження автентичності користувача через кілька незалежних факторів. MFA знижує ймовірність несанкціонованого доступу до мережі навіть у разі компрометації одного з факторів автентифікації. Крім того, методи шифрування, такі як WPA3, допомагають захистити дані під час передачі через мережу.

Актуальність даної роботи полягає в тому, що з кожним роком збільшується кількість кібератак на бездротові мережі. Захист даних і доступу до систем є критично важливим, особливо з урахуванням глобальних тенденцій переходу на дистанційну роботу та збільшення обсягу переданих даних через бездротові мережі.

Таким чином, дослідження в області захисту бездротових мереж за допомогою багатофакторної автентифікації є актуальним і необхідним для забезпечення високого рівня безпеки мережевих інфраструктур.

1 АНАЛІЗ СТАНДАРТІВ ТА ОСОБЛИВОСТЕЙ РОБОТИ БЕЗДРОТОВИХ МЕРЕЖ

Цей розділ присвячений огляду особливостей функціонування бездротових мереж, їх класифікації, стандартів та основних технологій, що використовуються для передачі даних. Виконання цього розділу спрямоване на вирішення завдання аналізу існуючих підходів до проєктування бездротових мереж, що необхідно для визначення найефективніших методів захисту.

У ході аналізу досліджено сучасні стандарти (зокрема, сімейство IEEE 802.11) та їх вплив на продуктивність і безпеку мереж. Отримані результати слугуватимуть базою для впровадження технологій захисту, розглянутих у наступних розділах.

1.1 Поняття та використання технології бездротової мережі Wi-Fi

Цей підрозділ описує основи функціонування бездротових мереж, їхнє місце у сучасному інформаційному середовищі, а також основні сфери застосування.

Бездротова мережа – це тип мережі, яка передає дані між пристроями без використання фізичних проводів, за допомогою радіохвиль або інших бездротових технологій, таких як інфрачервоне або мікрохвильове випромінювання.

Пристрої в такій мережі підключені один до одного або до Інтернету, що забезпечує зручність і мобільність користувачів.

Wi-Fi (Wireless Fidelity) – це технологія бездротового зв'язку, що дозволяє пристроям підключатися до інтернету або локальної мережі без використання

фізичних кабелів. Wi-Fi базується на стандартах бездротової передачі даних IEEE 802.11, що забезпечують стабільне з'єднання на основі радіочастотного спектру. З моменту свого створення Wi-Fi став ключовою технологією для мобільного зв'язку, домашніх і корпоративних мереж, а також мереж у громадських місцях.

Технологія Wi-Fi використовує радіочастоти, зазвичай в діапазонах 2,4 ГГц і 5 ГГц. Останні стандарти, такі як Wi-Fi 6 (802.11ax), також підтримують частоти 6 ГГц, що дозволяє зменшити перешкоди і підвищити пропускну здатність мережі.

Wi-Fi працює на основі передачі даних у формі радіохвиль між пристроями, що можуть виступати як точки доступу (Access Point, AP) або клієнтські пристрої (наприклад, ноутбуки, смартфони).

Точка доступу є проміжною ланкою між користувацькими пристроями та інтернетом чи іншими мережевими ресурсами. Для забезпечення безпеки даних використовуються різні методи шифрування, такі як WPA2 або новіший WPA3.

Бездротові Wi-Fi-мережі (стандарт IEEE 802.11) стали невід'ємною частиною сучасного світу завдяки своїй простоті розгортання, відносно низькій вартості та зручності у використанні.

Ці фактори сприяють постійному зростанню кількості WLAN, що призводить до збільшення щільності радіомереж. Однак зі збільшенням кількості пристроїв, що підключаються до Wi-Fi-мереж, зростають і ризики безпеки, пов'язані з несанкціонованим доступом та кіберзагрозами [5].

Мережі Wi-Fi використовуються не лише для доступу до Інтернету, але й для різноманітних додатків, таких як фінансові транзакції, передача конфіденційних даних, управління розумними пристроями та корпоративні комунікації. Ці сфери потребують високого рівня безпеки та захисту від несанкціонованого доступу.

1.2 Класифікація бездротових мереж

Розглядається поділ бездротових мереж за дальністю дії (PAN, LAN, MAN, WAN) та технологіями (Wi-Fi, Zigbee, Bluetooth, WiMAX).

Бездротові мережі поділяються на кілька категорій залежно від зони покриття, призначення та використовуваних технологій. Кожна з цих категорій має свої особливості та сфери застосування. Основними видами бездротових мереж є (рис. 1.1).

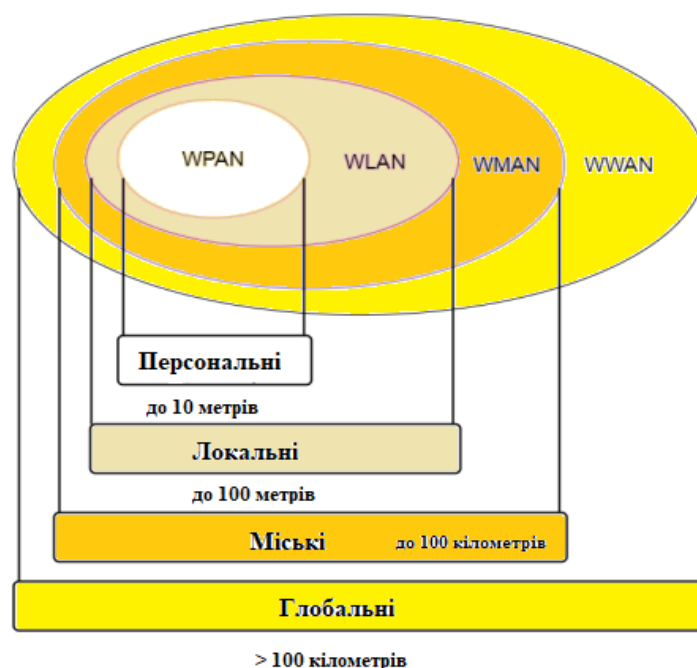


Рисунок 1.1 - Дальність дії бездротових мереж передачі даних

WLAN – це мережі, що забезпечують бездротовий зв'язок між пристроями в обмеженій географічній зоні, зазвичай в межах будівлі або кількох десятків метрів. Вони використовують стандарти IEEE 802.11, найвідоміший з яких — Wi-Fi. WLAN дозволяє обмінюватися даними між пристроями, такими як комп'ютери, смартфони та принтери, без потреби у кабелі [14].

WLAN (Wireless Local Area Network) – бездротова локальна мережа:

- діапазон покриття: до 100 метрів (залежить від середовища);

- призначення: забезпечення бездротового доступу до локальної мережі або інтернету в межах приміщення чи будівлі;
- технології: Wi-Fi (802.11 a/b/g/n/ac/ax);
- приклади застосування: домашні мережі, офісні мережі, публічні Wi-Fi зони;
- переваги: висока пропускна здатність, простота розгортання;
- недоліки: потреба в захисті від перехоплення даних, обмежений радіус дії.

WPAN – це мережі, що призначені для зв'язку між пристроями в особистій зоні, зазвичай на відстані до кількох метрів. Прикладами є технології Bluetooth і ZigBee, які використовуються для передачі даних між пристроями на невеликих відстанях, таких як навушники, розумні годинники або контролери "розумного будинку".

WPAN (Wireless Personal Area Network) – бездротова персональна мережа:

- діапазон покриття: до 10 метрів;
- призначення: забезпечення з'єднання між персональними пристроями на невеликій відстані;
- технології: Bluetooth, Zigbee, інфрачервоний зв'язок;
- приклади застосування: з'єднання між смартфонами, смарт-годинниками, навушниками, клавіатурами, мишами та іншими портативними пристроями;
- переваги: низьке енергоспоживання, простота підключення;
- недоліки: обмежений діапазон та пропускна здатність.

WMAN – це мережі, що охоплюють великі міські або регіональні території, забезпечуючи бездротовий зв'язок між великими групами користувачів. Вони використовуються для з'єднання мереж у різних будівлях або районах міста. Однією з відомих технологій є WiMAX, яка надає високошвидкісний доступ до Інтернету на відстанях до кількох десятків кілометрів.

Діапазон покриття: до 50-100 км. Це залежить від типу технології, що

використовується. Наприклад, технології на основі стандарту WiMAX можуть покривати відстані до 50 км у сільських районах і до 10 км у міських через вищу щільність будівель та інші перешкоди.

Тому в типових умовах міської забудови можна орієнтуватися на максимальний радіус дії до 50 км, а в ідеальних умовах (сільські райони з мінімумом перешкод) – до 100 км.

WMAN (Wireless Metropolitan Area Network) – бездротова міська мережа:

- призначення: об'єднання кількох локальних мереж у межах міста або регіону;
- технології: WiMAX (802.16), міські Wi-Fi мережі;
- приклади застосування: міські бездротові мережі для громадського доступу, корпоративні мережі;
- переваги: велика зона покриття, висока швидкість передачі даних;
- недоліки: високі витрати на розгортання, залежність від інфраструктури.

WWAN охоплюють великі географічні території, такі як країни або континенти, використовуючи технології стільникового зв'язку (3G, 4G, 5G) для передачі даних. Вони дозволяють підключення до Інтернету на великих відстанях і використовуються для мобільного доступу до мережі за межами традиційної інфраструктури WLAN чи WMAN.

WWAN (Wireless Wide Area Network) – бездротова глобальна мережа:

- діапазон покриття: кілька тисяч кілометрів;
 - призначення: забезпечення з'єднання на великих відстанях, часто між містами або країнами;
 - технології: мобільні мережі 2G/3G/4G/5G, супутниковий зв'язок;
 - приклади застосування: мобільний інтернет, супутникові комунікації.
- Україні прикладами операторів мереж WWAN можуть служити Київстар, Lifecell, Vodafone;
- переваги: можливість покриття великих відстаней, підтримка

мобільних користувачів;

- недоліки: високі затрати, залежність від операторів зв'язку, можливі перешкоди у зв'язку.

Стандарти бездротових мереж визначають правила та специфікації, за якими відбувається передача даних між пристроями без використання кабелів. Ці стандарти розробляються різними організаціями, такими як IEEE (Institute of Electrical and Electronics Engineers), 3GPP (Third Generation Partnership Project), Wi-Fi Alliance та інші. Вони забезпечують сумісність між пристроями різних виробників і гарантують стабільну роботу мереж у різних умовах. Стандарти бездротових мереж можна класифікувати за кількома ознаками, такими як область застосування, діапазон частот, швидкість передачі даних та технології [17].

1.3 Аналіз сучасних стандартів та технологій бездротових мереж

Цей підрозділ присвячений стандартам сімейства IEEE 802.11 та їхній еволюції. Окремо розглядаються технології Wi-Fi EasyMesh та Zigbee.

1.3.1 Стандарти сімейства IEEE 802.11

Стандарти сімейства IEEE 802.11 стосуються бездротових локальних мереж (Wireless Local Area Networks, WLAN) і визначають специфікації для передачі даних за допомогою радіохвиль. Це один із найпоширеніших стандартів для бездротових мереж, відомий завдяки популярним Wi-Fi технологіям. Всі стандарти цього сімейства визначають різні аспекти передачі даних, зокрема швидкість, частотний діапазон та методи доступу.

З моменту своєї появи в 1997 році ці стандарти постійно оновлювалися для підвищення швидкості передачі даних, збільшення радіусу дії та покращення енергоефективності та безпеки. Кожна версія стандарту має свої унікальні особливості, які роблять її придатною для різних сценаріїв використання [13].

Перший стандарт 802.11 Wi-Fi, прийнятий у 1997 році, забезпечував

швидкість передачі даних до 2 Мбіт/с і працював у частотному діапазоні 2.4 ГГц. Через низьку швидкість передачі та обмежений радіус дії стандарт не отримав широкого використання і був швидко оновлений.

Стандарт 802.11a працював у частотному діапазоні 5 ГГц і забезпечував швидкість передачі даних до 54 Мбіт/с. Через вищі частоти 802.11a забезпечував кращу продуктивність у щільних міських середовищах, де багато перешкод у діапазоні 2.4 ГГц. Однак менший радіус дії та вища вартість обладнання обмежили його популярність.

Працюючи в частотному діапазоні 2.4 ГГц, стандарт 802.11b забезпечував швидкість передачі даних до 11 Мбіт/с. Він став значно популярнішим завдяки низькій вартості обладнання та більшій зоні покриття. Однак через використання того ж діапазону частот, що і побутові прилади (наприклад, мікрохвильові печі), виникали проблеми з перешкодами.

Стандарт 802.11g поєднував переваги 802.11b (робота на частоті 2.4 ГГц) і високу швидкість 802.11a (до 54 Мбіт/с). Він швидко став популярним завдяки зворотній сумісності з обладнанням 802.11b.

802.11n став великим кроком уперед у розвитку Wi-Fi, оскільки підтримував роботу в обох частотних діапазонах (2.4 ГГц і 5 ГГц) і забезпечував швидкість до 600 Мбіт/с завдяки використанню технології MIMO (Multiple Input Multiple Output). Це дозволяло передавати кілька потоків даних одночасно, що значно підвищувало пропускну здатність мережі [20].

Стандарт 802.11ac працює лише в діапазоні 5 ГГц і підтримує швидкість до 1.3 Гбіт/с. Він використовує ширші канали (до 160 МГц), технологію MU-MIMO (Multi-User MIMO) і забезпечує ефективне використання радіоспектра, дозволяючи обслуговувати кілька користувачів одночасно. Технологія формування променя дозволяє антенам зосереджувати радіосигнали в напрямку конкретного пристрою, підвищуючи ефективність передачі даних. Одним із важливих нововведень стандарту 802.11ac стала підтримка багатокористувацького MIMO (MU-MIMO).

Тоді як звичайний MIMO направляє кілька потоків даних до одного клієнта,

MU-MIMO дозволяє передавати просторові потоки одночасно на кілька пристроїв. Це не підвищує швидкість окремих клієнтів, але збільшує загальну пропускну здатність мережі, підвищуючи її ефективність для всіх підключених користувачів.

802.11ax, також відомий як Wi-Fi 6, працює в обох частотних діапазонах (2.4 ГГц і 5 ГГц) і підтримує швидкість до 9.6 Гбіт/с. Основні переваги Wi-Fi 6 включають покращену продуктивність у середовищах з високою щільністю користувачів, завдяки використанню технологій OFDMA (Orthogonal Frequency Division Multiple Access) на рисунку 1.2 наведено та Target Wake Time (TWT) для зниження енергоспоживання пристроїв.

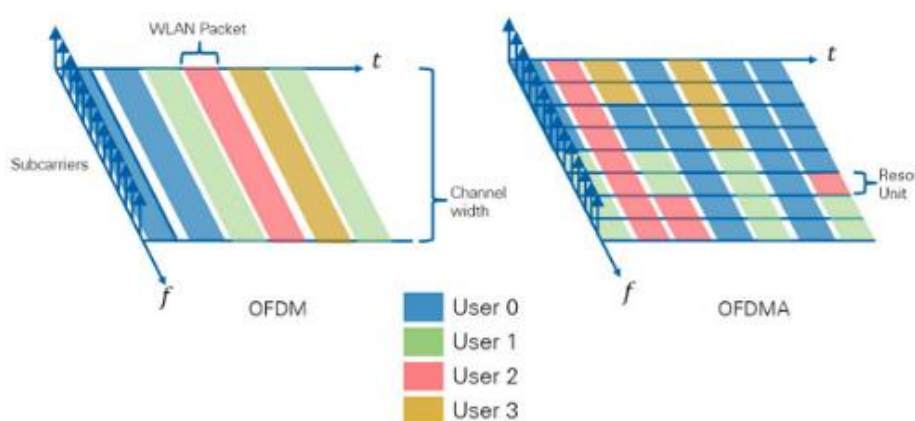


Рисунок 1.2 –Технології OFDM та OFDMA

На відміну від попередніх стандартів, Wi-Fi 6 дозволяє маршрутизатору обслуговувати більше антен, що дозволяє підключати більше пристроїв одночасно. Це забезпечує значно кращу продуктивність мережі як вдома, так і в громадських місцях. Однією з ключових інновацій Wi-Fi 6 є впровадження технології OFDMA (множинний доступ з ортогональним частотним розділенням каналів), яка покращує спектральну ефективність і дозволяє точці доступу встановлювати одночасні з'єднання з кількома користувачами, розділяючи спектр на менші підканали.

Wi-Fi 6 також дозволяє пристроям, що його підтримують, завантажувати

інформацію у чотири рази швидше та передавати її на сервер у шість разів швидше, порівняно з попередніми стандартами. Це забезпечує значний приріст швидкості та загальної продуктивності мережі.

Wi-Fi 6 підтримує технологію MU-MIMO (Multi-User Multiple-Input, Multiple-Output) для передачі даних у напрямку аплінку (від клієнта до маршрутизатора). У попередньому стандарті Wi-Fi 5 MU-MIMO працював лише в напрямку від маршрутизатора до клієнта (DL MIMO).

Wi-Fi 6, в теорії, здатен підтримувати одночасну передачу до восьми просторових потоків у обох напрямках (8x8) (рис. 1.3), а також доставляти до чотирьох потоків одному клієнту одночасно.

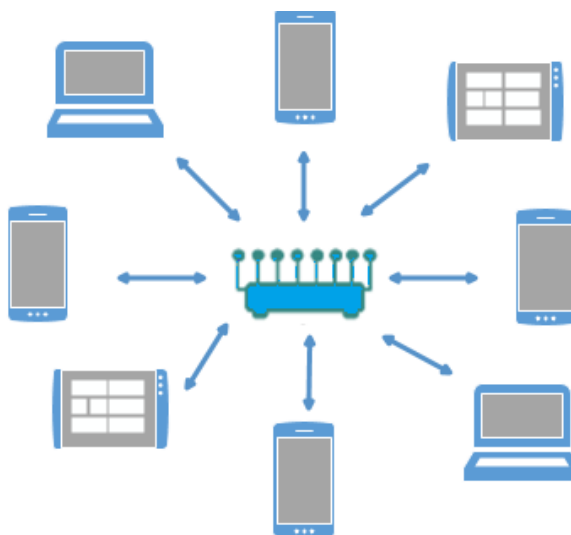


Рисунок 1.3 – Передача до 8 просторових потоків в обох напрямках

Однак на початкових етапах впровадження цієї технології можливості деякого обладнання з підтримкою 802.11ax можуть обмежуватися. Більшість пристроїв у масовому сегменті використовуватимуть конфігурації MIMO 4x4 або 2x2.

В таблиці 1.1 наведено порівняння стандартів IEEE 802.11.

Таблиця 1.1 – Порівняння стандартів IEEE 802.11

Стандарт	Рік прийняття	Частотний діапазон	Максимальна швидкість	Технології
802.11	1997	2.4 ГГц	2 Мбіт/с	DSSS
802.11a	1999	5 ГГц	54 Мбіт/с	OFDM
802.11b	1999	2.4 ГГц	11 Мбіт/с	DSSS
802.11g	2003	2.4 ГГц	54 Мбіт/с	OFDM
802.11n	2009	2.4 / 5 ГГц	600 Мбіт/с	MIMO, OFDM
802.11ac	2013	5 ГГц	1.3 Гбіт/с	MU-MIMO
802.11ax	2019	2.4 / 5 ГГц	9.6 Гбіт/с	OFDMA, MU-MIMO

1.3.2 Технологія Zigbee

Zigbee – це бездротовий стандарт для мереж з низьким енергоспоживанням і малою пропускну здатністю. Він працює на частоті 2.4 ГГц і забезпечує швидкість передачі даних до 250 Кбіт/с. Zigbee використовує технологію DSSS для передачі даних і має радіус дії до 100 метрів.

Zigbee часто використовується в системах "розумного дому", промисловій автоматизації та інших сферах, де важливо забезпечити довготривалу роботу пристроїв від батарей. Приклади застосування включають дистанційне керування освітленням, системи безпеки та моніторинг енергії.

1.3.3 Технологія WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) – це технологія, призначена для забезпечення бездротового широкосмугового доступу на великих відстанях. Вона здатна охоплювати значні території (до 50 км) і забезпечувати пропускну здатність до 70 Мбіт/с. WiMAX є стандартом для мереж MAN (Metropolitan Area Network), що робить його корисним для підключення сільських районів і великих міських агломерацій [1].

WiMAX застосовується для забезпечення високошвидкісного інтернету в районах, де дротовий зв'язок важко або дорого встановити. Він використовується як альтернатива для DSL та інших широкосмугових технологій.

1.3.4 Технологія Bluetooth

Bluetooth – це бездротова технологія для короткодистанційної передачі даних між пристроями, що працює в діапазоні 2.4 ГГц. Bluetooth дозволяє створювати персональні мережі PAN і підтримує швидкості до 3 Мбіт/с [6].

Bluetooth використовує технологію FHSS (Frequency Hopping Spread Spectrum), що знижує ризик перешкод від інших пристроїв, які працюють на тій же частоті. Останні версії технології підтримують більш ефективну роботу та підвищену швидкість.

1.3.5 Технологія Bluetooth Low Energy

Bluetooth Low Energy (BLE) є енергоефективною версією Bluetooth, яка призначена для пристроїв з низьким енергоспоживанням, як фітнес-трекери, датчики та пристрої Інтернету речей (IoT). BLE забезпечує економію енергії, одночасно підтримуючи стабільну передачу даних на коротких відстанях [7].

Кожна з описаних технологій має свої унікальні переваги та сфери застосування, що робить їх важливими для розвитку бездротових мереж у різних середовищах.

1.4 Опис моделі захисту бездротових мереж

На схемі представлена функціональна модель захисту бездротових мереж (рис. 1.4), яка забезпечує підвищену безпеку користувачів завдяки використанню багатофакторної автентифікації та системи шифрування даних [15].

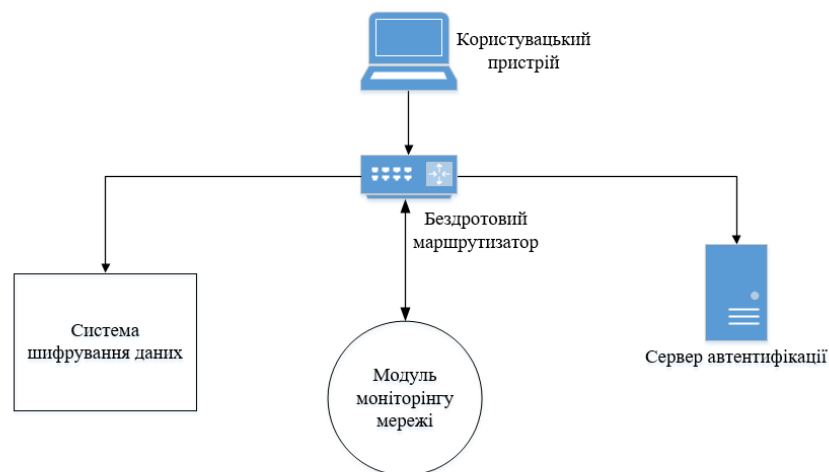


Рисунок 1.4 – Модель захисту

Користувачський пристрій:

- це початковий компонент у системі, який ініціює з'єднання з бездротовою мережею. Пристрій може бути представлений у вигляді смартфона, планшета, ноутбука або іншого гаджета, який має бездротовий модуль зв'язку;
- під час підключення користувач проходить процедуру автентифікації, що забезпечує захист від несанкціонованого доступу.

Бездротовий маршрутизатор:

- центральний елемент схеми, який виступає в ролі комунікаційного вузла між користувацьким пристроєм і внутрішньою мережею. Він забезпечує передачу даних та їх захист за допомогою вбудованих функцій шифрування, таких як WPA3;
- відповідає за маршрутизацію запитів на сервер автентифікації, обробку з'єднань та керування доступом до мережі.

Сервер автентифікації:

- виконує функцію перевірки особи користувача за допомогою багатофакторної автентифікації (MFA). Це може бути сервер RADIUS, який здійснює перевірку логінів, паролів та додаткових факторів, таких як SMS-коди, біометричні дані або апаратні токени;

- після успішної автентифікації сервер надає користувачеві доступ до мережі, що мінімізує ризики несанкціонованого доступу.

Система шифрування даних:

- забезпечує безпечну передачу інформації між користувацьким пристроєм і бездротовим маршрутизатором. Використовуються сучасні методи шифрування, такі як AES-256, які запобігають перехопленню та розшифруванню даних злоумисниками;

- вона інтегрована в маршрутизатор або може бути додатковим програмним чи апаратним модулем, який відповідає за шифрування та дешифрування переданих даних.

Модуль моніторингу мережі:

- відповідає за постійний моніторинг мережевого трафіку з метою виявлення аномалій та потенційних загроз. Цей модуль може використовувати методи аналізу поведінки та сигнатурного виявлення атак для забезпечення своєчасного реагування на інциденти;

- інформація про підозрілу активність передається адміністратору мережі для прийняття необхідних заходів.

Переваги запропонованої моделі:

- підвищена безпека: використання багатфакторної автентифікації значно знижує ризик несанкціонованого доступу до мережі;

- конфіденційність даних: завдяки шифруванню переданої інформації забезпечується захист від перехоплення та маніпуляцій з даними;

- моніторинг та виявлення загроз: модуль моніторингу дозволяє оперативно виявляти потенційні атаки та зменшувати ризик втрати даних.

Ця модель є гнучкою та може бути адаптована до різних умов і вимог користувачів, а також легко інтегрується в існуючу інфраструктуру бездротових мереж.

1.5 Постановка завдань

Реалізація та впровадження системи захисту бездротових мереж із використанням багатофакторної автентифікації потребує комплексного підходу до забезпечення безпеки і захисту переданих даних у бездротових мережах. На основі аналізу сучасних загроз безпеці та технологій автентифікації, можна визначити ключові задачі, які повинні бути вирішені під час виконання цього проєкту:

- аналіз вразливостей бездротових мереж: визначення основних загроз безпеці бездротових мереж (атаки типу "людина посередині", перехоплення даних та інші) і аналіз їх впливу на мережеву інфраструктуру;
- огляд та порівняння методів багатофакторної автентифікації та шифрування: оцінка різних методів автентифікації (двофакторна, багатофакторна) та шифрування, їхнього застосування в бездротових мережах та вплив на рівень безпеки;
- впровадження моделі захисту бездротових мереж: побудова моделі, що включає шифрування даних та багатофакторну автентифікацію для забезпечення надійного захисту користувачів і мережі;
- впровадження шифрування даних: вибір та інтеграція надійних методів шифрування для захисту переданої інформації у бездротовій мережі;
- реалізація механізмів багатофакторної автентифікації: проєктування механізмів автентифікації, що включають кілька рівнів перевірки ідентичності користувачів, таких як паролі, біометричні дані, смс-коди або апаратні токени;
- інтеграція з існуючою мережею: забезпечення сумісності впровадженної системи з поточними бездротовими мережами та пристроями, щоб гарантувати безперебійну роботу мережі після впровадження нових методів захисту;
- аналіз ефективності впроваджених методів: проведення порівняння

впровадженій системи з іншими методами захисту мережі для оцінки її ефективності у різних сценаріях використання та умовах експлуатації.

Ці задачі охоплюють усі етапи проєктування: від аналізу загроз і технологій захисту до впровадження і тестування багатофакторної автентифікації. Результатом буде створена ефективна система захисту бездротової мережі з багаторівневими механізмами автентифікації та шифруванням, яка гарантуватиме підвищений рівень безпеки даних у мережі.

2 АНАЛІЗ БЕЗПЕКИ ТА ТЕХНОЛОГІЙ ЗАХИСТУ БЕЗДРотовИХ МЕРЕЖ

Метою цього розділу є аналіз існуючих загроз, уразливостей та методів захисту, які застосовуються для забезпечення безпеки в бездротових мережах. На основі поставлених завдань виконано огляд основних видів атак, таких як DDoS, атаки типу "людина посередині" (MitM), атаки на рівні автентифікації та інші.

Також досліджено методи шифрування даних, зокрема стандарти WEP, WPA, WPA2, WPA3, що забезпечують конфіденційність переданої інформації. Завершенням розділу є обґрунтування оптимального методу захисту на основі порівняння їх ефективності.

2.1 Головні види атак на бездротові мережі

Бездротові мережі, завдяки своїй зручності та мобільності, стають все більш популярними. Проте ця популярність також супроводжується підвищенням

ризиків, пов'язаних із безпекою. Зловмисники постійно шукають способи атакувати бездротові мережі через їх вразливості, що пов'язані з фізичною природою радіосигналів та особливостями автентифікації.

Атаки на бездротові мережі можуть відбуватися з різних причин:

- викрадення даних: зловмисники можуть намагатися викрасти конфіденційну інформацію, таку як паролі, банківські реквізити чи особисті дані, для фінансової вигоди або для шантажу;
- незаконний доступ: хакери можуть шукати способи підключитися до бездротової мережі для несанкціонованого використання ресурсів, таких як інтернет-з'єднання, або для створення інших злочинних схем;
- шкода репутації: атаки на мережі можуть призвести до збоїв у роботі компаній або організацій, що може негативно вплинути на їхню репутацію;
- політичні чи ідеологічні мотиви: кібератаки можуть спрямовані на організації чи особистостей з метою висловлення протесту або досягнення певних цілей.

Існує кілька основних категорій атак, які загрожують безпеці бездротових мереж:

- несанкціонований доступ;
- атаки типу "людина посередині" (Man-in-the-Middle);
- атаки на мережеве обладнання;
- DDoS (Distributed Denial of Service);
- атака KRACK;
- атаки на рівні автентифікації.

2.1.1 Несанкціонований доступ до бездротової мережі

Несанкціонований доступ – це процес, коли зловмисник отримує доступ до бездротової мережі без відома або дозволу її власника. Це може відбуватися через різні методи, такі як злом паролів, експлуатація вразливостей у протоколах безпеки, або через використання відсутності належного захисту.

Підбір паролів тут зловмисники можуть використовувати програми для

автоматичного підбору паролів, намагаючись вгадати ключ доступу до мережі. Це можливо, якщо пароль є слабким або загальнодоступним.

Використання WPS (Wi-Fi Protected Setup). Багато маршрутизаторів мають функцію WPS, яка дозволяє легко підключати пристрої до мережі. Проте, якщо ця функція неправильно налаштована або використовує стандартний PIN, вона може стати вразливою для атак.

Атаки на шифрування, зловмисники можуть намагатися зламати старі протоколи шифрування, такі як WEP, які мають відомі вразливості. Використання сучасних методів шифрування, таких як WPA3, може зменшити ризик таких атак.

Соціальна інженерія зловмисники можуть спробувати обманути користувачів, щоб отримати доступ до їх облікових даних, використовуючи фішинг або інші методи маніпуляції.

Використання фальшивих точок доступу, а саме зловмисники створюють підроблені точки доступу, які мають таку ж назву, як легітимна мережа. Користувачі можуть підключатися до цих точок, надаючи зловмиснику можливість перехоплювати їх дані.

Отримавши доступ до бездротової мережі, зловмисники можуть:

- викрадати дані: це можуть паролі, фінансові реквізити та інша чутлива інформація.
- контролювати трафік: зловмисники можуть моніторити та аналізувати дані, що передаються через мережу.
- розповсюджувати шкідливе програмне забезпечення: після отримання доступу до мережі, зловмисники можуть розповсюджувати віруси або трояни на пристрої, що підключені до цієї мережі.
- використовувати мережу для злочинних дій: зловмисники можуть використовувати ресурси мережі для атак на інші системи або для незаконних дій.

Несанкціонований доступ є серйозною загрозою для бездротових мереж, яка може призвести до викрадення даних і зловживання ресурсами. Впровадження надійних заходів безпеки та регулярний моніторинг мережі є

критично важливими для захисту від цих атак.

2.1.2 Атаки типу "людина посередині" (MitM)

Атака типу "людина посередині" (MitM) (рис. 2.1) є серйозною загрозою для безпеки бездротових мереж і комп'ютерних систем. Вона відбувається, коли зловмисник перехоплює, контролює або модифікує зв'язок двома сторонами, що спілкуються, без відома жодної з них. Це дозволяє зловмиснику читати або змінювати інформацію, передається, ставши посередником у передачі даних [19].

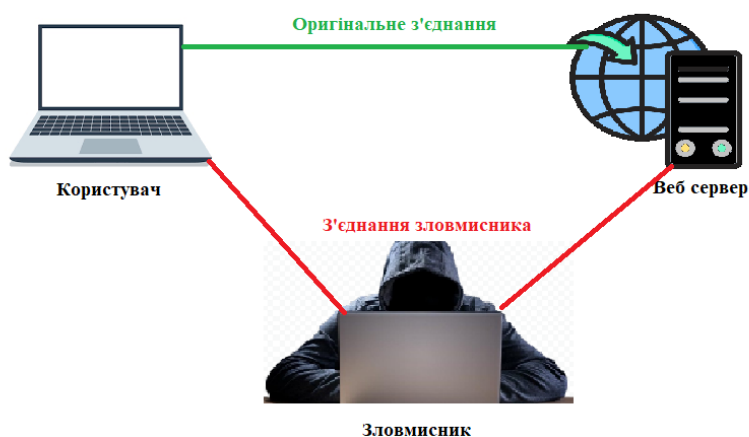


Рисунок 2.1 – Схема типової атаки Man-in-the-Middle

Атака типу "людина посередині" (MitM) часто включає два ключових етапи: перехоплення і розшифрування даних.

На етапі перехоплення зловмисник отримує доступ до даних, що передаються між двома сторонами. Цей процес може відбуватися кількома способами:

- створення фальшивої точки доступу де зловмисник налаштовує підроблену Wi-Fi мережу, схожу на легітимну, щоб привернути увагу користувачів;
- ARP Spoofing тут зловмисник підмінює MAC-адреси в таблицях ARP, перенаправляючи трафік до свого пристрою;
- DNS Spoofing відповіді DNS змінюються для перенаправлення користувачів на фальшиві сайти, що дозволяє перехоплювати їхні дані.

Після перехоплення трафіку зловмисник може спробувати розшифрувати зашифровані дані, щоб отримати доступ до конфіденційної інформації. Цей етап може включати [18]:

- використання вразливостей у шифруванні: Зловмисник намагається зламати протоколи шифрування, такі як WEP, або обходить HTTPS;
- SSL Stripping: Зловмисник усуває шифрування, змушуючи користувача підключатися через незахищене HTTP;
- дешифрування даних: За допомогою методів, таких як брутфорс, зловмисник намагається розшифрувати перехоплену інформацію.

Успішне перехоплення та розшифрування даних можуть призвести до серйозних наслідків, таких як: викрадення особистої інформації (логіни, паролі, фінансові дані). Неправомірне використання конфіденційних даних для шахрайства.

2.1.3 Атаки на мережеве обладнання

Ці атаки можуть проявлятися через фізичне втручання в обладнання, зокрема злом точок доступу та маршрутизаторів, що дозволяє зловмисникам змінювати налаштування та отримувати несанкціонований доступ до мережі.

Крім фізичних атак, зловмисники можуть експлуатувати вразливості в програмному забезпеченні мережевих пристроїв. Це може включати використання відомих вразливостей для отримання доступу до мережі або встановлення шкідливого програмного забезпечення, яке контролює мережу. Атаки типу "відмова в обслуговуванні" (DoS) також є поширеним методом, при якому зловмисник намагається перевантажити ресурси маршрутизатора шляхом надсилання великої кількості запитів, що призводить до збоїв у роботі.

Важливо також зазначити, що зловмисники можуть атакувати протоколи управління, використовуючи техніки, такі як ARP Spoofing і DNS Spoofing, що дозволяє їм перенаправляти трафік та викрадати дані. Наслідки цих атак катастрофічні, включаючи викрадення конфіденційної інформації, фінансові втрати та збої в роботі мережі.

2.1.4 Атаки типу DDoS (Distributed Denial of Service)

Атаки типу DDoS (Distributed Denial of Service) (рис.2.2) є одним із найпоширеніших і небезпечних методів, які використовуються зловмисниками для унеможливлення доступу до онлайн-сервісів, веб-сайтів або мережевих ресурсів. Основною метою таких атак є перевантаження системи або мережі великою кількістю запитів, що призводить до зниження продуктивності або повного збою в роботі [2].

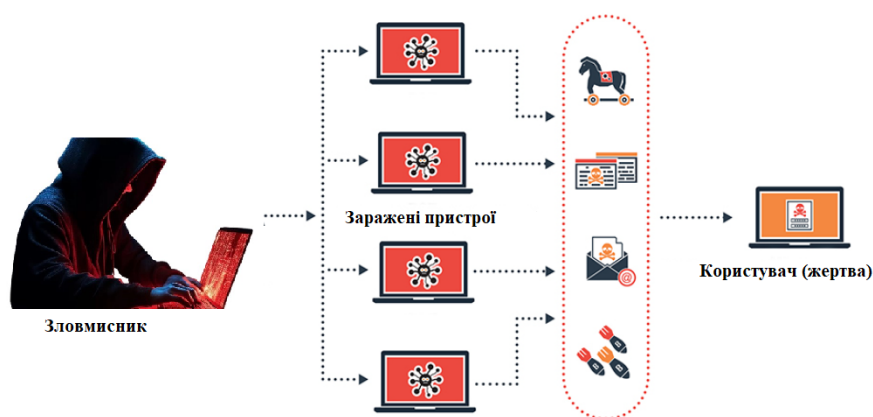


Рисунок 2.2 – Схема DDoS-атаки

Атаки DDoS здійснюються шляхом координації великої кількості з'єднань, які надсилають запити до цільового ресурсу. Це може відбуватися через:

- ботнети: зловмисники використовують мережу скомпрометованих пристроїв (ботнетів), щоб надсилати одночасні запити до цілі. Ботнет може складатися з тисяч або навіть мільйонів заражених комп'ютерів, які працюють без відома їхніх власників;
- злом серверів: атаки здійснені шляхом зламу серверів, на яких працює цільовий ресурс. Наприклад, зловмисник може використати вразливості в програмному забезпеченні для підключення до сервера та надсилання великої кількості запитів;
- стрес-тестування: деякі атаки можуть імітувати легітимний трафік, щоб обманути системи захисту та призвести до перевантаження ресурсів.

Атаки DDoS можна розділити на кілька типів:

- об'ємні атаки: ці атаки намагаються перевантажити пропускну здатність мережі, надсилаючи великий обсяг трафіку. Прикладом є атаки з використанням UDP flood або ICMP flood;
- атаки на рівні протоколів: ці атаки намагаються перевантажити сервери або мережеві пристрої, використовуючи вразливості на рівні протоколів. Наприклад, SYN flood атакує процес встановлення з'єднання TCP;
- атаки на рівні додатків: цей тип атак намагається перевантажити сервер, на якому працює веб-додаток, шляхом надсилання специфічних запитів, які вимагають великих ресурсів.
- Наприклад, HTTP flood може згенерувати тисячі запитів до конкретної веб-сторінки.

Атаки типу DDoS можуть мати серйозні наслідки для організацій:

- втрата доступу до послуг: атака може призвести до недоступності веб-сайту або онлайн-сервісів для легітимних користувачів;
- фінансові втрати: недоступність послуг може призвести до значних фінансових збитків, особливо для бізнесу, що покладається на онлайн-операції;
- пошкодження репутації: постраждалі організації можуть втратити довіру клієнтів, що може вплинути на їхню репутацію на ринку.

DDoS-атаки залишаються серйозною загрозою для бездротових мереж та онлайн-сервісів. Знання методів проведення таких атак та їх наслідків є важливими для забезпечення безпеки інформаційних систем. Організації повинні вживати проактивні заходи для захисту від DDoS-атак.

2.1.5 Атака типу KRACK

Атака KRACK (Key Reinstallation Attack) — це одна з найбільш небезпечних загроз для бездротових мереж, що використовують стандарт WPA2. Вперше описана в 2017 році, ця уразливість дозволяє зломисникам перехоплювати та маніпулювати трафіком бездротової мережі, навіть якщо вона захищена надійним паролем.

KRACK є результатом уразливостей у протоколі WPA2, що виникають під час реалізації чотиристороннього рукостискання (4-way handshake), яке використовується для встановлення з'єднання між точкою доступу та клієнтом. У процесі атаки зловмисник повторно надсилає пакети, які містять ключ шифрування. Це змушує клієнт повторно встановлювати той самий ключ шифрування, що дозволяє зловмиснику дешифрувати трафік.

Механізм атаки KRACK:

- чотиристороннє рукостискання: у процесі встановлення з'єднання точка доступу та клієнт обмінюються ключами шифрування. В рамках цього обміну клієнт генерує новий сеансовий ключ для кожного з'єднання;
- повторне встановлення ключа: зловмисник перехоплює та повторно надсилає третій пакет рукостискання, що змушує клієнтський пристрій використовувати той самий ключ шифрування повторно;
- дешифрування даних: після повторного встановлення ключа зловмисник отримує можливість перехоплювати трафік, оскільки клієнтський пристрій починає використовувати вже відомий ключ для шифрування та дешифрування.

Наслідки атаки KRACK:

- перехоплення даних: зловмисник може отримати доступ до незашифрованої інформації, такої як паролі, повідомлення, електронна пошта та конфіденційні файли;
- маніпуляція трафіком: атака дозволяє вносити зміни в трафік, наприклад, впроваджувати шкідливі програми або перенаправляти користувачів на фішингові сайти;
- зниження довіри до WPA2: попри високий рівень безпеки WPA2, атака KRACK продемонструвала, що навіть найсучасніші стандарти можуть мати критичні уразливості.

2.1.6 Атаки на рівні автентифікації

Автентифікація є ключовим етапом захисту бездротових мереж, оскільки

саме вона визначає, хто отримує доступ до мережі. Однак атаки на цьому рівні можуть серйозно підірвати безпеку мережі, що дозволяє зловмисникам отримати несанкціонований доступ до мережі та її ресурсів. Основні вразливості пов'язані з використанням слабких паролів, однакових облікових даних для багатьох облікових записів і застосуванням методів брутфорс.

Одна з найпоширеніших вразливостей на рівні автентифікації — це використання користувачами слабких або передбачуваних паролів. Багато користувачів надають перевагу паролям через зручність, що значно полегшує зловмисникам їх підбір. Слабкими паролями вважаються короткі або прості комбінації, наприклад:

- "123456";
- "password";
- "admin123";
- або навіть використання власних імен чи днів народження.

Зловмисники можуть легко підібрати подібні паролі, використовуючи автоматизовані інструменти для підбору, а це призводить до несанкціонованого доступу до мережі. Після отримання доступу вони можуть контролювати трафік, перехоплювати дані або навіть знищити систему безпеки мережі.

Користувачі часто використовують один і той самий пароль або облікові дані для різних сервісів. Це створює додаткову вразливість, адже якщо один із цих сервісів скомпрометовано, зловмисники можуть отримати доступ до інших ресурсів, використовуючи ті самі облікові дані.

Використання однакових паролів для різних мереж або онлайн-сервісів збільшує ризик для користувачів і організацій, оскільки успішний злом однієї системи може автоматично означати злом багатьох інших.

Цей вид загрози часто використовується у так званих атаках "credential stuffing", коли вкрадені облікові дані використовуються для масового доступу до різних сервісів.

Брутфорс — це метод атаки, при якому зловмисник використовує

автоматизовані інструменти для спроби підбору пароля шляхом перебору всіх можливих комбінацій символів. Брутфорс-атаки особливо ефективними проти коротких і слабких паролів, оскільки такі паролі легко зламуються за допомогою сучасних обчислювальних потужностей.

Методи брутфорс включають:

- прямий брутфорс: перебір можливих паролів до знаходження правильного;
- словникові атаки: використання списків із поширених або передбачуваних паролів;
- гібридні атаки: поєднання технік словникових атак із модифікаціями (наприклад, додавання цифр або спеціальних символів до простих паролів).

Якщо пароль є занадто коротким або недостатньо складним, метод брутфорс дуже ефективним, і зловмисник може отримати доступ до мережі за короткий час. Це особливо небезпечно для мереж, які не використовують методи багатофакторної автентифікації (MFA), оскільки один пароль часто є єдиною перешкодою для зловмисника.

Популярні паролі залишаються одними з найлегших для злому, незважаючи на зростання кіберзагроз. У першій половині 2022 року понад 53 мільйони громадян США стали жертвами кіберінцидентів, згідно з даними AAG.

В таблиці 2.1 наведено найпоширеніші паролі 2023 року.

Таблиця 2.1 – Топ-20 найпоширеніших паролів 2023 року

Ранг	Пароль	Час необхідний для злому	Кількість разів використання
1	123456	< 1 секунди	4,52 млн
2	admin	< 1 секунди	4 млн
3	12345678	< 1 секунди	1,37 млн
4	123456789	< 1 секунди	1,21 млн
5	1234	< 1 секунди	969,8 тис
6	12345	< 1 секунди	728,4 тис
7	password	< 1 секунди	710,3 тис
8	123	< 1 секунди	528,1 тис
9	Aa123456	< 1 секунди	319,7 тис
10	1234567890	< 1 секунди	302,7 тис

Продовження таблиці 2.1

Ранг	Пароль	Час необхідний для злому	Кількість разів використання
11	UNKNOWN	17 хвилин	240,4 тис
12	1234567	< 1 секунди	234,2 тис
13	123123	< 1 секунди	224,3 тис
14	111111	< 1 секунди	191,4 тис
15	Password	< 1 секунди	177,7 тис
16	12345678910	< 1 секунди	172,5 тис
17	000000	< 1 секунди	168,7 тис
18	admin123	11 секунд	159,4 тис
19	*****	< 1 секунди	152,5 тис
20	user	1 секунда	146,2 тис

Статистика показує, що 17 із 20 найпоширеніших паролів можуть стати зламани менш ніж за секунду. Це стосується як простих цифрових комбінацій, так і «оригінальних» паролів на кшталт "password" та "administrator".

Паролі типу "user" ламаються за секунду, а "admin123" — за 11 секунд. Лідер списку — пароль "UNKNOWN", який зламається за 17 хвилин.

Цікаво, що пароль "admin", який у 2022 році опинився на другій позиції, раніше не входив навіть до топ-200 за останні п'ять років. А пароль "123456" чотири з п'яти разів утримував перше місце як найпопулярніший, лише один раз поступившись паролю "password".

2.2 Методи забезпечення безпеки бездротових мереж

2.2.1 Огляд методів шифрування

Бездротові мережі, завдяки своїй зручності та мобільності, стають все більш популярними. Проте ця популярність також супроводжується підвищенням ризиків, пов'язаних із безпекою.

Зловмисники постійно шукають способи атакувати бездротові мережі через їх вразливості, що пов'язані з фізичною природою радіосигналів та особливостями

автентифікації [10].

WEP (Wired Equivalent Privacy) став першим стандартом шифрування для Wi-Fi мереж, представленим у 1999 році. Його розроблено для забезпечення конфіденційності даних, еквівалентної дротовим мережам Ethernet. Попри революційний характер на той час, WEP дуже швидко став вразливим до атак через недосконалість реалізації [21].

Технічні характеристики WEP:

- алгоритм шифрування: RC4 (потоківий шифр);
- довжина ключа: 40 біт (основний режим) або 104 біти (розширений режим);
- вектор ініціалізації (IV): додає 24 біти до ключа, утворюючи загальний розмір ключа 64 або 128 біт.

Кожен пакет даних шифрується за допомогою поєднання секретного ключа та випадкового вектора ініціалізації. WEP також використовує CRC32 для перевірки цілісності пакетів, однак цей механізм не забезпечує достатнього рівня захисту.

Вразливості WEP:

- повторення векторів ініціалізації: через коротку довжину IV (24 біти) вектори повторюються, особливо в мережах із високим трафіком, що дозволяє зловмисникам дешифрувати дані.
- статичний ключ: один ключ використовується для всіх пристроїв у мережі, що створює серйозну загрозу в разі його компрометації.
- алгоритм RC4: алгоритм має слабкості, що дозволяють відновити ключ через атаки методом перебору.

WPA (Wi-Fi Protected Access) був представлений у 2003 році як тимчасове рішення для заміни WEP. Основна мета WPA полягала в усуненні недоліків WEP без необхідності заміни обладнання.

Технічні характеристики WPA:

- алгоритм шифрування: RC4 (як і у WEP), але з використанням

протоколу TKIP (Temporal Key Integrity Protocol);

- динамічне оновлення ключів: TKIP генерує новий ключ для кожного пакета даних, що усуває проблему статичних ключів WEP;
- перевірка цілісності: WPA впровадив механізми перевірки автентичності даних для виявлення змін у пакетах.

Переваги WPA:

- динамічна зміна ключів значно ускладнила атаки на повторювані ключі;
- механізми перевірки цілісності зменшили ризики модифікації пакетів.

Недоліки WPA:

- обмеження RC4: алгоритм RC4 продовжує залишатися основною слабкістю WPA;
- вразливість до атак Beck-Tews: ця атака дозволяє дешифрувати WPA-трафік протягом кількох хвилин.

WPA більше не використовується в сучасних мережах і замінений WPA2.

WPA2 (Wi-Fi Protected Access II) впроваджений у 2004 році, став стандартом безпеки для бездротових мереж протягом багатьох років.

Цей протокол суттєво вдосконалив механізми шифрування та автентифікації, усунувши обмеження WPA.

Технічні характеристики WPA2:

- алгоритм шифрування: AES (Advanced Encryption Standard) із довжиною ключа 128 біт;
- протокол безпеки: CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol), що забезпечує автентифікацію та цілісність даних;
- режими роботи: Personal використовує Pre-Shared Key (PSK); Enterprise використовує сервер автентифікації RADIUS.

Переваги WPA2:

- використання AES зробило WPA2 практично недоступним для атак методом грубої сили [11];

- протокол CCMP забезпечив захист даних і запобігання їх модифікації.

Недоліки WPA2:

- уразливість до атак KRACK (Key Reinstallation Attack), що дозволяє перехоплювати трафік і виконувати його модифікацію;
- використання WPS (Wi-Fi Protected Setup) може бути скомпрометованим для отримання ключа PSK.

WPA2 залишається найпоширенішим стандартом, хоча його поступово замінює WPA3.

WPA3 (Wi-Fi Protected Access III) був впроваджений у 2018 році як еволюційний етап розвитку шифрування Wi-Fi. Цей стандарт усунув основні недоліки WPA2 і адаптувався до сучасних загроз у кіберпросторі [9].

Технічні характеристики WPA3:

- алгоритм шифрування: AES-GCM (Galois/Counter Mode), що підвищує криптографічну стійкість;
- протокол автентифікації: SAE (Simultaneous Authentication of Equals), який замінив PSK. SAE забезпечує стійкість до атак методом грубої сили;
- додаткові функції: OWE (Opportunistic Wireless Encryption), який захищає відкриті мережі без пароля та захист пристроїв IoT завдяки Easy Connect.

Переваги WPA3:

- індивідуальне шифрування кожного з'єднання;
- покращена захищеність навіть за використання слабких паролів;
- висока сумісність із сучасними пристроями.

Недоліки WPA3:

- необхідність сучасного обладнання;
- високі витрати на оновлення інфраструктури.

WPA3 є рекомендованим стандартом Wi-Fi Alliance для всіх нових мереж.

В таблиці 2.2 наведено порівняння методів шифрування.

Таблиця 2.2 – Порівняння методів шифрування

Метод	Рік впровадження	Алгоритм впровадження	Довжина ключа	Рівень безпеки	Особливості	Недоліки
WEP	1999	RC4	40/104 біт	Низький	Статичний ключ, короткий IV	Вразливий до атак на повторення IV
WPA	2003	RC4 + TKIP	128 біт	Середній	Динамічний ключ, перевірка цілісності	Уразливий до атак Beck-Tews
WPA2	2004	AES + CCMP	128 біт	Високий	Надійне шифрування, режими Personal і Enterprise	Уразливий до атак KRACK
WPA3	2018	AES-GCM + SAE	192 біт	Дуже високий	Захист у відкритих мережах, Easy Connect	Необхідність сучасного обладнання

2.2.2 Вибір та обґрунтування оптимального методу шифрування

На основі аналізу методів шифрування, представлених у попередньому підрозділі, визначено, що WPA3 є найкращим вибором для забезпечення захисту бездротових мереж.

Цей стандарт поєднує сучасні технології шифрування та аутентифікації, що значно підвищують рівень безпеки порівняно з попередніми методами. Нижче наведено критерії вибору та обґрунтування рішення [3].

Високий рівень безпеки WPA3 усуває вразливості попередніх версій (WEP, WPA, WPA2) і забезпечує сучасний рівень захисту завдяки таким ключовим удосконаленням:

- протокол SAE (Simultaneous Authentication of Equals): замінює PSK (Pre-Shared Key), забезпечуючи стійкість до атак перебору пароля навіть при слабких паролях [22];
- Forward Secrecy: забезпечує унікальність кожного сеансу шифрування, що захищає попередні дані навіть у разі компрометації ключів;
- захист від атак типу "dragonblood", характерних для WPA2.

Покращений захист у відкритих мережах. WPA3 включає функцію Opportunistic Wireless Encryption (OWE), яка шифрує дані навіть у відкритих мережах без введення пароля. Це значно підвищує рівень безпеки для публічних точок доступу.

Сумісність з попередніми версіями. Хоча WPA3 є новим стандартом, він передбачає зворотну сумісність із WPA2, що дозволяє поступовий перехід на нову технологію без суттєвих змін у мережевій інфраструктурі.

Підтримка 192-бітового шифрування. WPA3-Enterprise забезпечує ще вищий рівень безпеки за рахунок використання 192-бітового ключа, відповідного стандартам Commercial National Security Algorithm (CNSA). Це робить його ідеальним для корпоративного середовища.

Захист IoT-пристроїв. WPA3 підтримує функцію Easy Connect, яка спрощує підключення пристроїв Інтернету речей (IoT), одночасно зберігаючи високий рівень безпеки.

Метод шифрування WPA3 є оптимальним вибором для забезпечення захисту бездротових мереж завдяки високому рівню безпеки, стійкості до сучасних атак, покращенню захисту в публічних мережах і підтримці IoT-пристроїв.

Незважаючи на необхідність оновлення інфраструктури, переваги WPA3 значно переважають, роблячи його найбільш перспективним стандартом для використання в сучасних і майбутніх мережах.

Для впровадження WPA3 у мережу необхідно:

- використовувати сучасні маршрутизатори та точки доступу, що підтримують WPA3;
- оновити прошивки на сумісних пристроях;
- впровадити індивідуальне шифрування сесій для кожного клієнта;
- використовувати OWE для захисту відкритих мереж.

На основі аналізу методів шифрування та враховуючи сучасні вимоги до безпеки, WPA3 є оптимальним вибором для захисту бездротових мереж.

Його впровадження забезпечить високий рівень захисту, стійкість до атак і адаптивність до майбутніх викликів, роблячи цей стандарт найкращим рішенням для сучасних мереж.

2.2.3 Методи багатфакторної автентифікації

MFA працює на основі трьох основних факторів:

- щось, що ви знаєте (паролі, пін-коди або секретні питання);
- щось, що ви маєте (смартфони, токени, смарт-карти або додатки для генерації одноразових кодів (OTP));
- щось, чим ви є (біометричні дані, як-от відбитки пальців, розпізнавання обличчя чи сітківки ока) [8].

Одноразові паролі (OTP) є дійсними лише для одного сеансу або короткого проміжку часу.

Алгоритми генерації OTP:

- TOTP (Time-based OTP): Генерує паролі, прив'язані до часу [4];
- HOTP (HMAC-based OTP): Використовує хешування для генерації паролів.

Приклади використання: SMS, додатки (Google Authenticator, Microsoft Authenticator).

Переваги: простота впровадження та висока ефективність.

Недоліки: вразливість до атак на перехоплення повідомлень (SIM-свопінг).

Апаратні токени. Токени — це пристрої, які генерують одноразові коди або забезпечують доступ через NFC чи USB.

Типи токенів:

- генератори OTP (наприклад, YubiKey);
- смарт-карти.

Переваги: надійність і незалежність від зовнішніх каналів зв'язку.

Недоліки: додаткові витрати на обладнання.

Біометрична автентифікація використовує фізичні або поведінкові характеристики особи.

Приклади:

- відбиток пальця;
- розпізнавання обличчя чи сітківки ока;
- розпізнавання голосу.

Переваги: висока стійкість до компрометації.

Недоліки: можливі помилки розпізнавання, залежність від якісного обладнання.

Push-сповіщення. Користувач отримує сповіщення на свій мобільний пристрій і підтверджує автентифікацію натисканням кнопки.

Приклади: Duo Mobile, Microsoft Authenticator.

Переваги: висока зручність і швидкість.

Недоліки: залежність від доступності Інтернету.

Геолокаційна автентифікація. Використання інформації про місцезнаходження для підтвердження особи.

Переваги: підвищення рівня безпеки за рахунок аналізу місця доступу.

Недоліки: вразливість до підробки геолокації.

Багатофакторна автентифікація на основі ризиків. Використовує динамічний підхід, оцінюючи ризики залежно від поведінки користувача (час входу, місце, пристрій тощо) [12].

Переваги: зменшує кількість зайвих перевірок для користувачів з низьким ризиком.

Недоліки: залежність від складних алгоритмів і аналітики.

В таблиці 2.3 наведено порівняння методів багатофакторної автентифікації.

Таблиця 2.3: Порівняння методів багатофакторної автентифікації

Метод автентифікації	Рівень безпеки	Зручність для користувача	Вартість впровадження	Основні вразливості
Паролі	Низький	Висока	Низька	Викрадення пароля, атаки грубою силою

Продовження таблиці 2.3

Метод автентифікації	Рівень безпеки	Зручність для користувача	Вартість впровадження	Основні вразливості
ОТР	Середній	Середня	Середня	Перехоплення коду через SMS
Апаратні токени	Високий	Середня	Висока	Втрата або крадіжка токена
Біометрія	Дуже високий	Висока	Висока	Злом або підробка біометричних даних

Механізми багатофакторної автентифікації значно підвищують рівень безпеки в сучасних інформаційних системах. Найпоширеніші методи - це одноразові паролі, апаратні токени, біометрія та push-сповіщення. Кожен із них має свої переваги та недоліки, тому оптимальний вибір залежить від специфіки системи. У сучасних умовах важливо впроваджувати багатофакторні підходи, що поєднують декілька методів, для забезпечення максимальної стійкості до атак.

3 ВПРОВАДЖЕННЯ СИСТЕМИ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ

Цей розділ спрямований на впровадження системи захисту, яка включає механізми шифрування даних (WPA3) та багатофакторну автентифікацію (MFA). Виконання цього розділу дозволяє досягти мети роботи, впроваджуючи методи захисту. У розділі представлено реалізація системи, алгоритми її роботи та детальне описання реалізації.

3.1 Впровадження шифрування даних

Підрозділ описує реалізацію WPA3 у бездротовій мережі.

Впровадження шифрування WPA3 у бездротову мережу є ключовим етапом захисту даних від несанкціонованого доступу. У цьому підрозділі детально описується процес інтеграції WPA3 в мережу, включаючи налаштування точки доступу, клієнтських пристроїв та перевірку ефективності шифрування. Схема налаштування зображена на рисунку 3.1 [15].

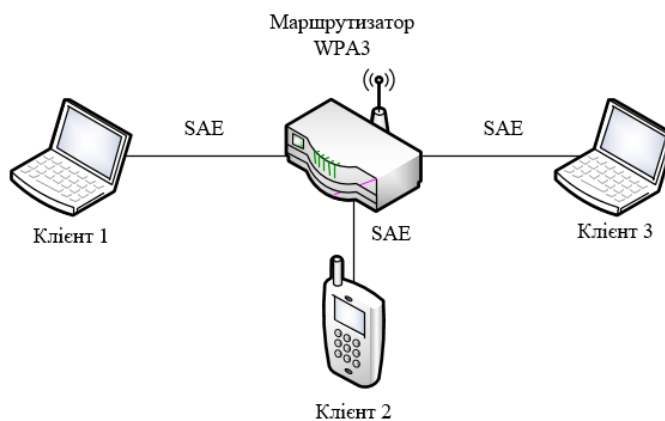


Рисунок 3.1 – Схема налаштування WPA3 у бездротовій мережі.

Оновлення мережевого обладнання. Для впровадження WPA3 необхідно переконатися, що точка доступу та клієнтські пристрої підтримують цей стандарт. Якщо обладнання не відповідає вимогам, слід оновити його прошивку або замінити на сумісне [9].

Налаштування точки доступу (маршрутизатора). Точка доступу є основним елементом бездротової мережі, через який передаються дані. Процес налаштування WPA3 включає:

Оновлення обладнання та програмного забезпечення:

- перевірка сумісності маршрутизатора та клієнтських пристроїв із WPA3;

- оновлення мікропрограми (firmware) маршрутизатора до останньої версії, яка підтримує WPA3;
- перевірка операційної системи клієнтських пристроїв на наявність підтримки WPA3 (наприклад, Windows 10+, Android 10+, iOS 13+).

Налаштування маршрутизатора (рис. 3.2):

- увійти в веб-інтерфейс маршрутизатора через IP-адресу (наприклад, 192.168.0.1);
- вибрати пункт меню "Налаштування бездротової мережі";
- у розділі "Безпека" вибрати WPA3-Personal або WPA3-Enterprise залежно від потреби;
- увімкнути протокол SAE (Simultaneous Authentication of Equals) для забезпечення захищеного обміну ключами;
- встановити надійний пароль для мережі (мінімум 12 символів, включаючи великі літери, цифри та спеціальні символи) зробив пароль з 20 символів, що дає велику надійність;
- зберегти налаштування та перезавантажити маршрутизатор та перевірити налаштування на пристрої.

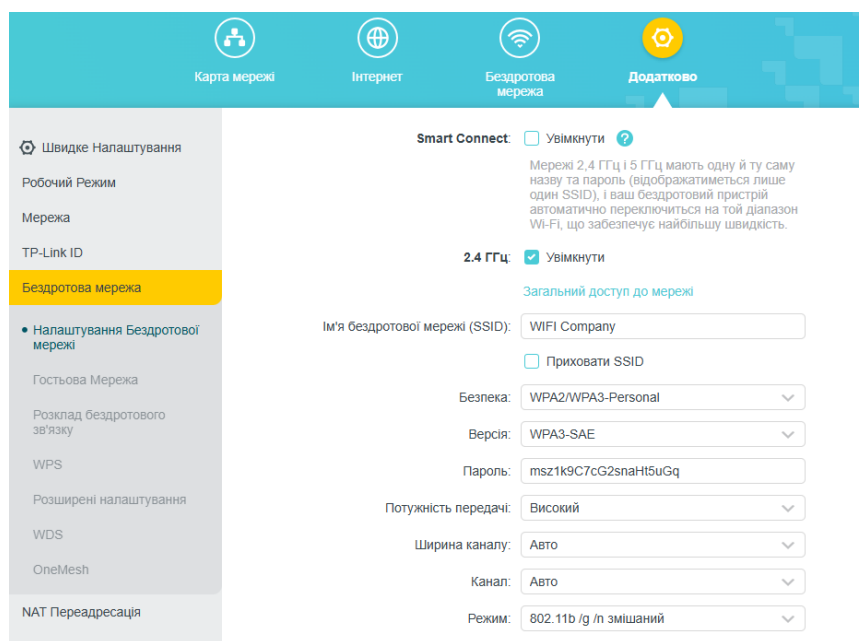


Рисунок 3.2 – Процес налаштування роутера

Налаштування клієнтських пристроїв (рис. 3.3):

- увійти в меню "Налаштування Wi-Fi" на клієнтському пристрої;
- знайти SSID мережі, що використовує WPA3;
- ввести пароль для підключення;
- перевірити, чи відображається підключення як захищене WPA3.

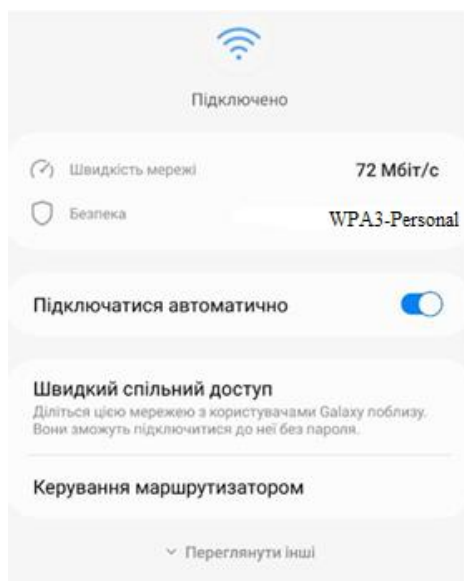


Рисунок 3.3 – Перевірка налаштування на пристрої

Інтеграція WPA3 у бездротову мережу дозволяє значно підвищити рівень безпеки, забезпечуючи захист даних від атак грубою силою та перехоплення. Налаштування цього стандарту є доступним і сумісним із більшістю сучасних пристроїв, що робить WPA3 оптимальним вибором для захисту як приватних, так і публічних мереж.

3.2 Реалізація механізмів багатофакторної автентифікації

Багатофакторна автентифікація (MFA) є одним із ключових методів захисту сучасних бездротових мереж, що дозволяє значно підвищити безпеку доступу до

мережі шляхом використання кількох рівнів перевірки ідентичності користувачів. MFA забезпечує додатковий рівень захисту, що є важливим у боротьбі з несанкціонованим доступом, перехопленням даних та іншими кіберзагрозами.

Для забезпечення високого рівня безпеки доступу до бездротових мереж пропонується система багатофакторної автентифікації (MFA), яка складається з кількох рівнів перевірки [16]. Така система базується на поєднанні різних факторів автентифікації: знань та володіння. У цьому підрозділі описано структуру системи, принципи її функціонування та сумісність із бездротовими мережами. Система автентифікації з кількома рівнями перевірки складається з різних компонентів (рис. 3.4).

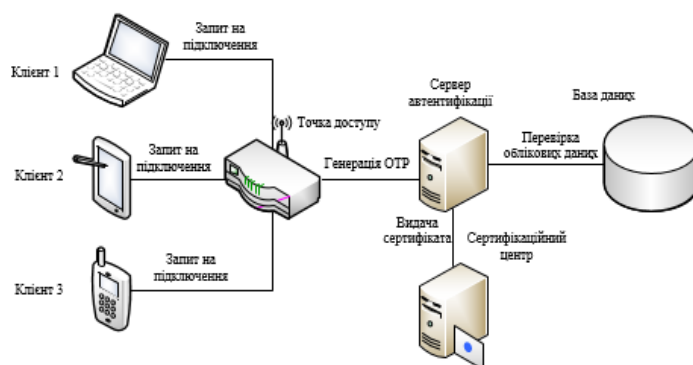


Рисунок 3.4 – Схема багатофакторної автентифікації

Клієнтський пристрій:

- мобільний телефон, ноутбук, планшет або інший пристрій, який використовується для доступу до мережі;
- встановлений додаток або веб-інтерфейс для взаємодії з системою автентифікації.

Сервер автентифікації:

- центральний елемент, який обробляє запити автентифікації, перевіряє облікові дані та взаємодіє з базою даних користувачів;
- реалізує механізми генерації одноразових паролів (OTP), аналізу біометричних даних та обробки push-сповіщень.

База даних користувачів: містить зашифровані облікові дані, біометричні шаблони, ключі шифрування та історію входів.

Безпроводова мережа: інфраструктура, яка включає точки доступу (Access Point) і маршрутизатори для підключення користувачів до мережі.

Сертифікаційний центр: видає цифрові сертифікати для забезпечення довіри між клієнтами та сервером автентифікації.

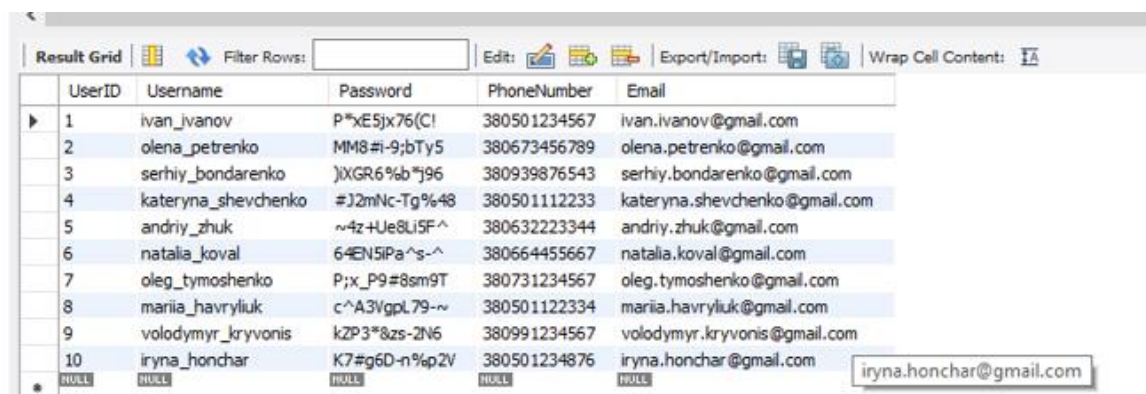
Для налаштування системи MFA пропонуються такі кроки:

Інтеграція серверу автентифікації:

- розгортання серверу автентифікації в існуючій інфраструктурі мережі;
- налаштування взаємодії серверу з точками доступу через протокол RADIUS (Remote Authentication Dial-In User Service).

Реєстрація користувачів (рис. 3.5):

- створення облікових записів у базі даних користувачів;
- в базу можуть бути внесені всі необхідні дані користувачів.



UserID	Username	Password	PhoneNumber	Email
1	ivan_ivanov	P*xE5jx76(CI	380501234567	ivan.ivanov@gmail.com
2	olena_petrenko	MM8#i-9;bTy5	380673456789	olena.petrenko@gmail.com
3	serhiy_bondarenko	)XGR6%b*j96	380939876543	serhiy.bondarenko@gmail.com
4	kateryna_shevchenko	#J2mNc-Tg%48	38050112233	kateryna.shevchenko@gmail.com
5	andriy_zhuk	~4z+Ue8U5F^	38063223344	andriy.zhuk@gmail.com
6	natalia_koval	64EN5Pa^s-^	380664455667	natalia.koval@gmail.com
7	oleg_tymoshenko	P;x_P9#8sm9T	380731234567	oleg.tymoshenko@gmail.com
8	maria_havryliuk	c^A3Vgpl.79-~	380501122334	maria.havryliuk@gmail.com
9	volodymyr_kryvonis	kZP3*&zs-2N6	380991234567	volodymyr.kryvonis@gmail.com
10	iryna_honchar	K7#g6D-n%p2V	380501234876	iryna.honchar@gmail.com

Рисунок 3.5 – Приклад таблиці з даними користувачів

Налаштування генерації ОТР, а саме впровадження алгоритмів ТОТР/НОТР для генерації паролів, що змінюються з кожним сеансом. Це забезпечує додатковий бар'єр проти несанкціонованого доступу та робить систему автентифікації значно стійкішою до сучасних атак.

При необхідності можна впровадити додатковий рівень автентифікації, а саме біометричні дані. Це рішення ідеально підходить для організацій, які

працюють із конфіденційною інформацією або вразливою інфраструктурою.

Впровадження механізму біометричної перевірки:

- інтеграція біометричних сканерів із сервером автентифікації;
- використання захищеного протоколу передачі даних для відправки біометричних шаблонів.

Тестування системи:

- перевірка працездатності кожного рівня автентифікації;
- виявлення можливих вразливостей та їх усунення.

Запропонований алгоритм процесу роботи багатофакторної автентифікації наведено нижче.

На початку зустрічає вітальна сторінка, на якій є кнопка за допомогою якої можна перейти до першого рівня автентифікації (рис. 3.6).

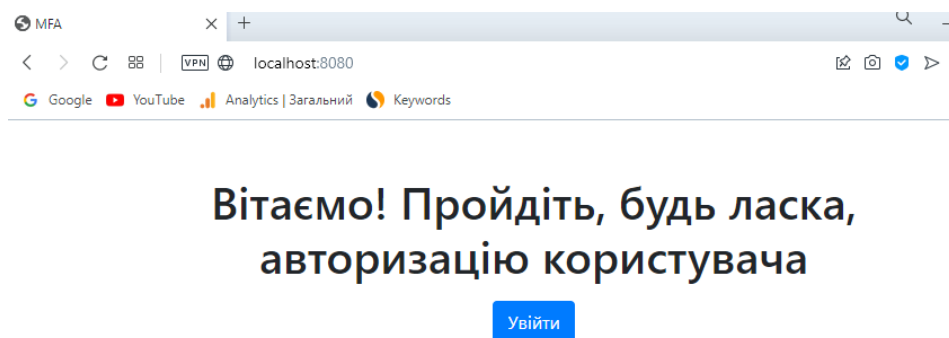


Рисунок 3.6 – Перша сторінка, яка зустрічає користувача

Перший рівень (пароль) (рис. 3.7, 3.8):

- користувач вводить унікальне ім'я користувача та пароль;
- сервер автентифікації перевіряє відповідність даних у базі;
- у разі успіху користувач переходить до наступного рівня перевірки, але якщо дані введені невірно то виводиться повідомлення про помилку.

На лістингу 3.1 можна побачити функцію, що відповідає за перевірку правильності введених користувачем облікових даних (логіна і пароля).

Лістинг 3.1 – Функція обробки авторизації користувачів

```
func handleLogin(w http.ResponseWriter, r *http.Request) {
    if r.Method == http.MethodGet {
        _ = tmpl.ExecuteTemplate(w, "login.html", nil)
        return
    }

    r.ParseForm()
    username := r.FormValue("username")
    password := r.FormValue("password")

    account, exists := userAccounts[username]
    if !exists || account.Pass != password {
        http.Redirect(w, r, "/login", http.StatusFound) //
        Перенаправлення при помилці
        return
    }

    if account.OTPSecret == "" {
        http.Redirect(w, r, "/generate-otp?username="+username,
        http.StatusFound)
        return
    }

    _ = tmpl.ExecuteTemplate(w, "validate.html", struct{ Name
    string }{Name: username})
}
```

Функція `handleLogin` отримує HTTP-запит і обробляє дані форми. Верифікація пароля відбувається шляхом порівняння введених даних із записами в базі `userAccounts`. У разі помилки користувач перенаправляється на сторінку авторизації, де виводиться повідомлення про помилку.



Рисунок 3.7 – Перший рівень автентифікації (пароль)

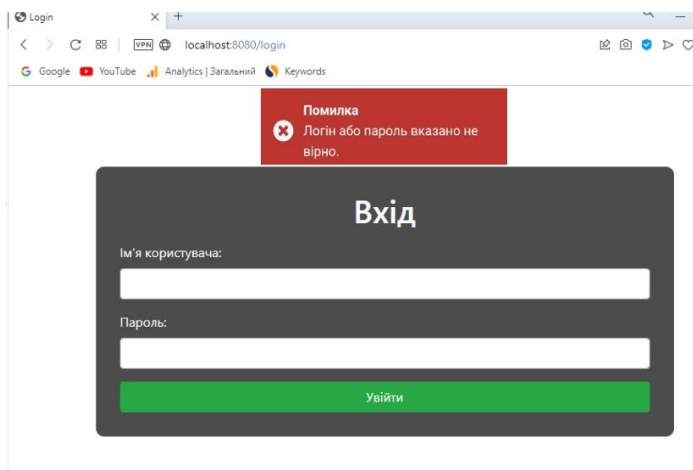


Рисунок 3.8 – Результат введення недостовірних даних

На другому рівні багатфакторної автентифікації (МФА) передбачається використання одноразового пароля (ОТР), що генерується динамічно за допомогою алгоритму TOTP (Time-based One-Time Password). Це дозволяє суттєво підвищити безпеку, оскільки кожен пароль діє лише протягом короткого періоду часу і є унікальним для кожного сеансу.

Навіть якщо зломисник отримає доступ до попереднього коду, він буде недійсним для наступних сеансів.

Другий рівень (одноразовий пароль) (рис. 3.9, 3.10):

- після успішного проходження першого рівня, користувач може побачити сторінку на якій буде зображено QR-код. Після сканування переходить на наступну сторінку;
- сервер автентифікації генерує ОТР за алгоритмом TOTP (Time-based One-Time Password);
- ОТР надсилається на мобільний пристрій користувача через мобільний додаток наприклад Google Authenticator.

Після успішного введення пароля сервер генерує одноразовий пароль (ОТР), який можна сканувати через QR-код у програмі. Реалізації можна побачити в лістингу 3.2.

Лістинг 3.2 – Функція генерації одноразового пароля

```
func createOTP(w http.ResponseWriter, r *http.Request) {
    username := r.URL.Query().Get("username")
    account, exists := userAccounts[username]
    if !exists {
        http.Redirect(w, r, "/", http.StatusFound)
        return
    }

    if account.OTPSecret == "" {
        secret, err := totp.Generate(totp.GenerateOpts{
            Issuer:      "SecureSystem",
            AccountName: username,
        })
        if err != nil {
            http.Error(w, "Unable to generate TOTP secret.",
http.StatusInternalServerError)
            return
        }
        account.OTPSecret = secret.Secret()
    }

    otpLink:=
    fmt.Sprintf("otpauth://totp/SecureSystem:%s?secret=%s&issuer=Se
cureSystem", username, account.OTPSecret)
    data := struct {
        OTPLink string
        Name     string
    }{
        OTPLink: otpLink,
        Name:    username,
    }
    _ = tmpl.ExecuteTemplate(w, "qrcode.html", data)
}
```

Ця функція `createOTP` створює секретний ключ для OTP та генерує посилання для його інтеграції в мобільні додатки (наприклад, Google Authenticator).

Генерується секретний ключ за допомогою бібліотеки `totp`. Якщо у користувача ще немає ключа, він створюється та зберігається у відповідному полі `OTPSecret`. Посилання у форматі `otpauth://` передається на сторінку з QR-кодом. Вихід: Відображення сторінки для сканування QR-коду.

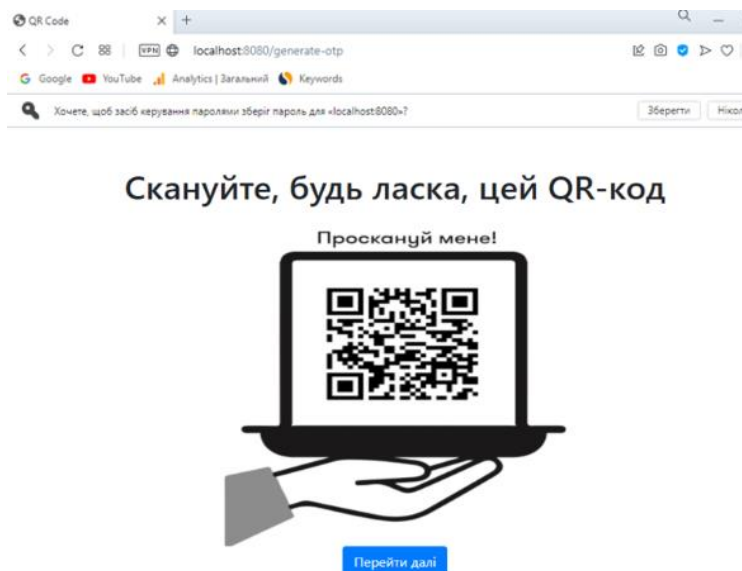


Рисунок 3.9 – Сканування для переходу

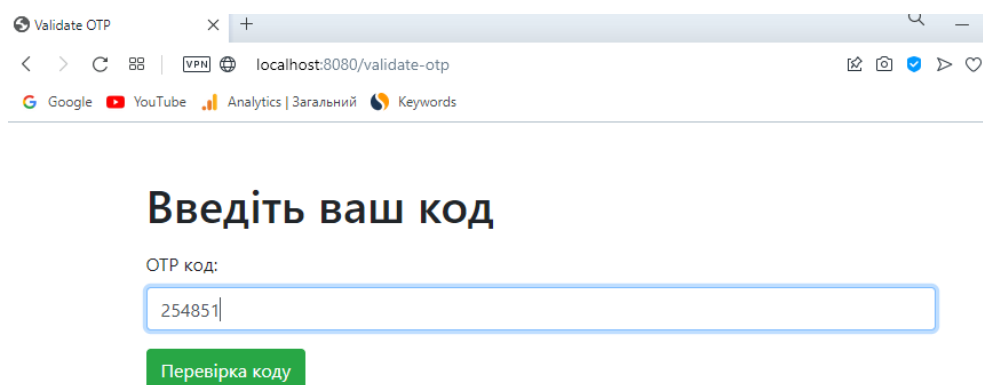


Рисунок 3.10 – Другий рівень автентифікації (ОТР)

Перевірка ОТР (рис. 3.11):

- користувач вводить ОТР у поле автентифікації, після чого сервер перевіряє його дійсність;
- при невірному вводі коду людина побачить помилку, яка буде означати, що потрібно перевірити чи правильно введено код.

На цьому етапі користувач вводить код ОТР, згенерований мобільним додатком. Сервер перевіряє його валідність. На лістингу 3.3 видно роботу програмного коду.

Лістинг 3.3 – Функція перевірки одноразового пароля

```
func checkOTP(w http.ResponseWriter, r *http.Request) {
    if r.Method == http.MethodPost {
        r.ParseForm()
        username := r.FormValue("username")
        otpCode := r.FormValue("otpCode")

        account, exists := userAccounts[username]
        if !exists {
            http.Error(w, "User not found",
http.StatusBadRequest)
            return
        }

        if totp.Validate(otpCode, account.OTPSecret) {
            http.SetCookie(w, &http.Cookie{
                Name: "loggedInUser",
                Value: username,
                Path: "/",
                MaxAge: 3600, // 1 година
            })
            http.Redirect(w, r, "/dashboard",
http.StatusSeeOther)
        } else {
            http.Redirect(w, r, "/validate-
otp?username="+username, http.StatusTemporaryRedirect)
        }
    }
}
```

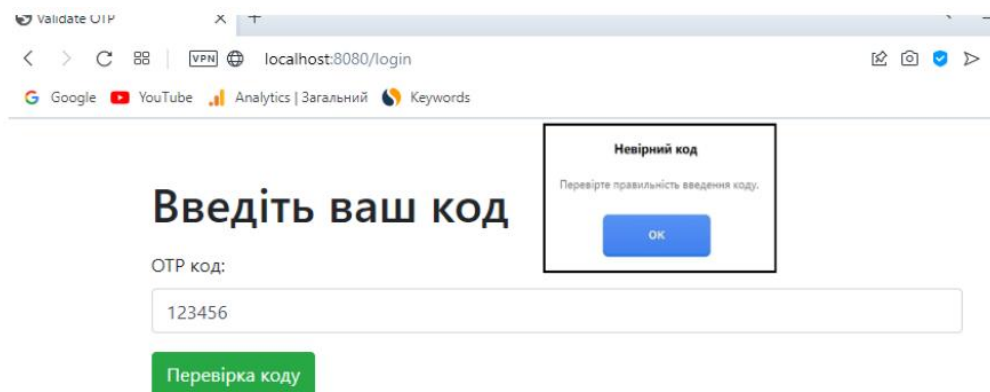


Рисунок 3.11 – Результат введення невірного коду (ОТР)

Авторизація (рис. 3.12): після успішного проходження всіх рівнів сервер автентифікації надсилає підтвердження точки доступу Wi-Fi, що користувач може підключитися до мережі.

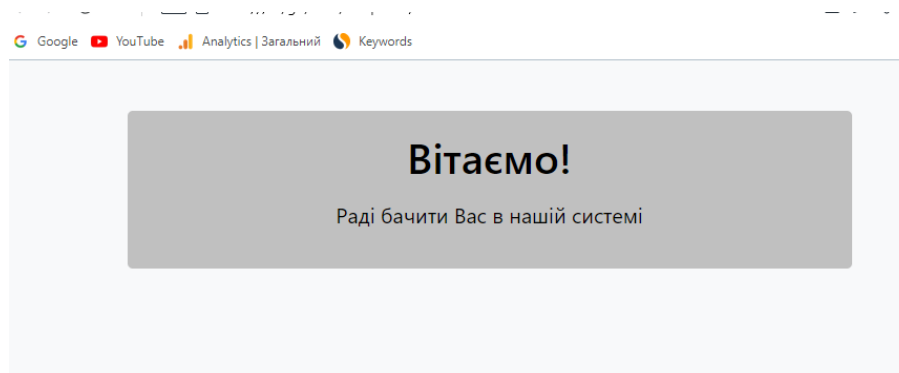


Рисунок 3.12 – Результат введення вірного коду (ОТР)

Система багатофакторної автентифікації складається з кількох рівнів перевірки: пароля, одноразового коду. Інтеграція з бездротовими мережами забезпечується через використання WPA3 та сучасних алгоритмів шифрування. Такий підхід гарантує високий рівень безпеки, сумісність із сучасними стандартами та зручність використання для кінцевих користувачів.

4 АНАЛІЗ ЕФЕКТИВНОСТІ ВПРОВАДЖЕНИХ МЕТОДІВ ЗАХИСТУ

Цей розділ присвячений оцінці ефективності впроваджених рішень із захисту бездротових мереж, зокрема, стандарту WPA3 та системи багатофакторної автентифікації (MFA). Основна мета цього розділу є порівняти запропоновану систему захисту з іншими методами, такими як WEP, WPA, WPA2, а також альтернативними методами автентифікації, зокрема однофакторною (1FA), двофакторною (2FA) та біометричною автентифікацією.

Результати тестування представлені у вигляді таблиць і графіків, що демонструють, як впровадження WPA3 та MFA впливає на загальну продуктивність і захист бездротової мережі в реальних умовах.

4.1 Оцінка впровадження WPA3 у бездротових мережах

У цьому підрозділі аналізується ефективність WPA3 порівняно з попередніми стандартами (WEP, WPA, WPA2). Виконується тестування швидкості передачі даних, затримки, стабільності з'єднання та рівня захисту від атак, таких як "людина посередині", DDoS та KRACK.

Стандарт WPA3 забезпечує сучасний рівень захисту бездротових мереж, завдяки новим алгоритмам шифрування та вдосконаленим механізмам автентифікації [20]. Для аналізу його ефективності проведено порівняння з попередніми стандартами (WEP, WPA, WPA2) за такими критеріями :

- рівень безпеки: відсоток атак, що вдалося запобігти;
- швидкість завантаження (Mbps): середня швидкість завантаження даних із сервера;
- швидкість відправлення (Mbps): середня швидкість передачі даних до сервера;
- затримка (ms): час, необхідний для передачі одного пакета між клієнтом і сервером;
- втрати пакетів (%): відсоток даних, що не дійшли до пункту призначення;
- час автентифікації (с): час, необхідний для підтвердження користувача;
- складність налаштування (шкала від 1 до 5, де 5 — дуже складно).

В таблиці 4.1 наведено результати впровадження WPA3 із попередніми стандартами.

Таблиця 4.1 - Порівняння WPA3 із попередніми стандартами

Параметр	WEP	WPA	WPA2	WPA3
Рівень безпеки, %	40%	70%	85%	98%
Швидкість завантаження, Mbps	48	70	90	88

Продовження таблиці 4.1

Параметр	WEP	WPA	WPA2	WPA3
Швидкість відправлення, Mbps	45	68	88	86
Затримка, ms	50	30	15	12
Втрати пакетів, %	5%	2.5%	1.8%	0.5%
Час автентифікації, с	1.5	1.8	2.0	2.2
Складність налаштування	1	2	3	3

Параметри WPA3:

- рівень безпеки: WPA3 використовує сучасний алгоритм автентифікації Simultaneous Authentication of Equals (SAE), який замінює PSK (Pre-Shared Key) у WPA2. SAE захищає від атак типу brute force навіть за умови слабких паролів. Завдяки Forward Secrecy кожна сесія має унікальний ключ, що робить неможливим розшифрування попереднього трафіку у разі компрометації ключа;
- швидкість завантаження та відправлення: WPA3 незначно впливає на швидкість завантаження (-2%) і відправлення даних (-2.3%) у порівнянні з WPA2, оскільки використовує обчислювально складніші алгоритми шифрування AES-GCM;
- затримка та втрати пакетів: затримка у WPA3 трохи більша (+2 мс) через додаткову перевірку шифрування. Однак втрати пакетів становлять лише 0.5%, що значно нижче, ніж у старіших стандартів, завдяки оптимізації передачі даних і зменшенню вразливостей;
- час автентифікації: використання SAE збільшує час автентифікації на 10% у порівнянні з WPA2 через додаткові криптографічні перевірки;
- складність налаштування: WPA3 вимагає оновлення маршрутизаторів і клієнтських пристроїв, сумісних із новим стандартом. Однак цей процес одноразовий і передбачає автоматичне налаштування більшості параметрів.

Рисунок 4.1 демонструє порівняння ефективності стандартів шифрування для бездротових мереж: WEP, WPA, WPA2 та WPA3, за ключовими параметрами,

зокрема швидкість завантаження, швидкість відправлення та затримка (ms).

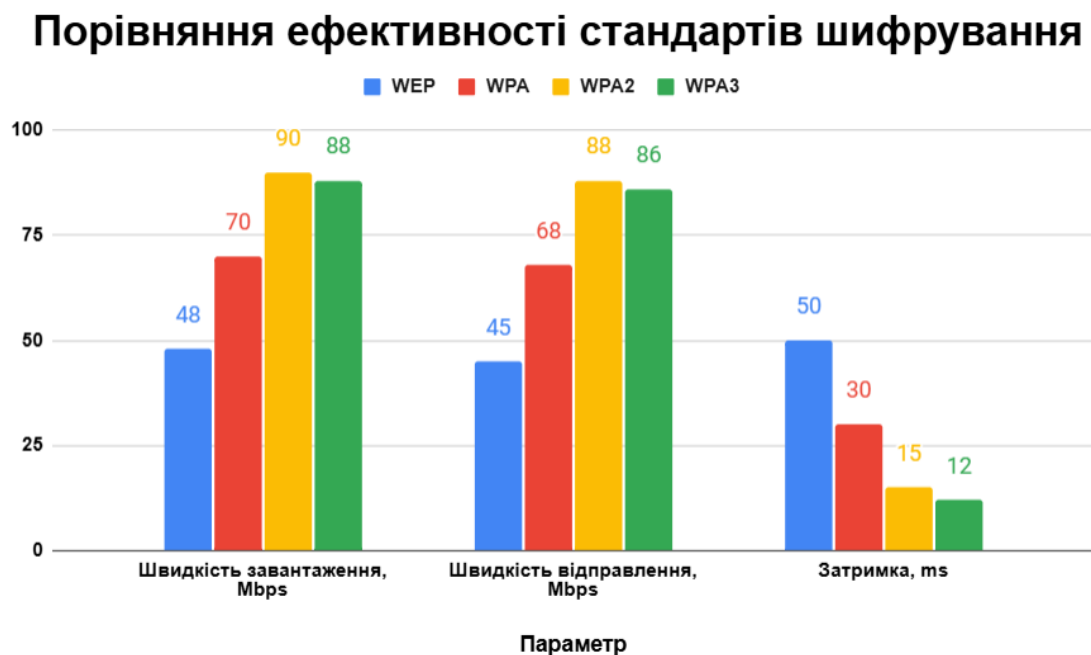


Рисунок 4.1 – Порівняння ефективності стандартів шифрування

Швидкість завантаження (Mbps):

- WEP демонструє найнижчу швидкість завантаження — 48 Mbps, що пояснюється застарілими алгоритмами шифрування;
- WPA забезпечує приріст до 70 Mbps, проте залишається нижчим за сучасні стандарти;
- WPA2 досягає 90 Mbps, що є піковим показником для стандартів;
- WPA3 трохи поступається WPA2, з показником 88 Mbps, через використання складніших алгоритмів шифрування.

Швидкість відправлення (Mbps):

- WEP показує результат 45 Mbps, що знову є найгіршим серед усіх стандартів;
- WPA підвищує цей показник до 68 Mbps, що демонструє вдосконалення;
- WPA2 забезпечує найвищий рівень швидкості — 88 Mbps;
- WPA3, як і в попередньому параметрі, трохи нижчий — 86 Mbps, що

також пов'язано з високим рівнем захисту.

Затримка (ms):

- WEP має найвищу затримку — 50 ms, що значно впливає на продуктивність мережі;
- WPA покращує цей показник до 30 ms, зменшуючи вплив шифрування на час передачі;
- WPA2 демонструє ще кращий результат — 15 ms;
- WPA3 забезпечує мінімальну затримку — 12 ms, що робить його найкращим стандартом у цьому показнику.

Результати аналізу:

- покращення безпеки: WPA3 забезпечує захист навіть у відкритих мережах через використання Opportunistic Wireless Encryption (OWE), що шифрує дані навіть без пароля;
- вплив на продуктивність: незначне зменшення швидкості та збільшення затримки є прийнятними для більшості сценаріїв використання.
- мінімальні втрати: оптимізація шифрування та передавання даних дозволяє уникнути більшості помилок передачі;
- сумісність: WPA3 підтримує зворотну сумісність із WPA2, що забезпечує поступовий перехід без заміни всього обладнання.

WPA3 - це найбільш сучасний і надійний стандарт шифрування, що забезпечує високий рівень безпеки без суттєвого впливу на продуктивність мережі. Його впровадження є доцільним для будь-яких середовищ із високими вимогами до безпеки.

WPA3, попри незначне зменшення швидкості завантаження та відправлення даних, забезпечує мінімальну затримку та високий рівень безпеки.

Ці дані підтверджують доцільність використання WPA3 для середовищ із високими вимогами до безпеки та продуктивності.

4.2 Оцінка впровадження MFA та порівняння з альтернативами

Підрозділ присвячений аналізу різних методів автентифікації, таких як MFA, 1FA, 2FA та біометрія. Оцінюється рівень безпеки, зручність використання, час автентифікації, вартість впровадження та доступність у разі збоїв. Результати подано у вигляді порівняльної таблиці та графіків, що дозволяють обґрунтувати переваги впровадження MFA в умовах сучасних кіберзагроз.

Багатофакторна аутентифікація (MFA) стала ключовим методом забезпечення кібербезпеки, який дозволяє значно підвищити захищеність систем шляхом поєднання декількох факторів автентифікації. Для оцінки ефективності MFA виконано порівняння з іншими методами автентифікації:

- однофакторна автентифікація (1FA): використання одного пароля;
- двофакторна автентифікація (2FA): комбінація пароля з додатковим фактором, наприклад, SMS-кодом;
- біометрична автентифікація: використання фізичних характеристик користувача (відбиток пальця, розпізнавання обличчя тощо).

До аналізу включено такі ключові показники:

- рівень безпеки (запобігання атакам, %): частка атак, які не змогли обійти механізми захисту;
- зручність використання (шкала 1–5): наскільки зручно користувачам виконувати автентифікацію;
- час автентифікації (секунди): середній час на виконання всіх етапів входу;
- складність впровадження (шкала 1–5): оцінка складності інтеграції системи в існуючу інфраструктуру;
- вартість впровадження та обслуговування (грн/користувача): середня вартість встановлення та підтримки технології для одного користувача;
- доступність у разі збоїв: як метод працює в умовах, коли один із

факторів стає недоступним (наприклад, відсутність мережі для SMS).

В таблиці 4.2 наведено результати впровадження MFA порівнянно з аналогами.

Таблиця 4.2 – Порівняння методів автентифікації

Параметр	1FA	2FA	Біометрія	MFA
Рівень безпеки (1–5)	2	4	4.5	5
Зручність використання (1–5)	5	3	4	3.5
Час автентифікації, сек.	5	10	8	12
Складність впровадження (1–5)	1	3	4	4.5
Вартість впровадження	Низька	Середня	Висока	Висока
Доступність у разі збоїв	Висока	Середня	Низька	Середня

Рівень безпеки:

- найвищу оцінку отримує 1FA (5 балів), оскільки користувачу достатньо ввести пароль;
- 2FA (3 бали) менш зручна через необхідність отримувати та вводити додаткові коди;
- біометрія (4 бали) є досить простою для кінцевого користувача, але вимагає спеціального обладнання;
- MFA (3.5 бали) забезпечує баланс між безпекою та зручністю, але процес автентифікації може займати більше часу.

Час автентифікації:

- 1FA вимагає найменше часу — 5 секунд, оскільки включає тільки введення пароля;
- 2FA займає в середньому 10 секунд, враховуючи очікування SMS або генерацію коду;
- біометрія скорочує час до 8 секунд, оскільки перевірка виконується автоматично;

- MFA потребує найбільше часу (12 секунд) через необхідність виконання кількох перевірок.

Складність впровадження:

- 1FA є найпростішим у налаштуванні (1 бал), адже вимагає лише створення бази даних паролів;

- 2FA має середню складність (3 бали) через інтеграцію додаткових сервісів (SMS, додатки);

- біометрія (4 бали) потребує спеціалізованого обладнання (сканерів відбитків, камер тощо);

- MFA (4.5 бала) вимагає інтеграції декількох систем автентифікації, що робить її найскладнішою у впровадженні.

Вартість впровадження:

- 1FA є найдешевшим методом;

- 2FA вимагає більшої інфраструктури, підвищуючи витрати;

- біометрія є найдорожчою через необхідність придбання спеціального обладнання;

- MFA має значну вартість через комплексність системи.

Доступність у разі збоїв:

- 1FA завжди доступна, оскільки не залежить від зовнішніх чинників;

- 2FA та MFA можуть бути недоступними у разі відсутності мережі (наприклад, для SMS-кодів);

- біометрія має найнижчу доступність через залежність від обладнання, яке може вийти з ладу.

На рисунку 4.2 можна побачити графік порівняння ефективності автентифікації.

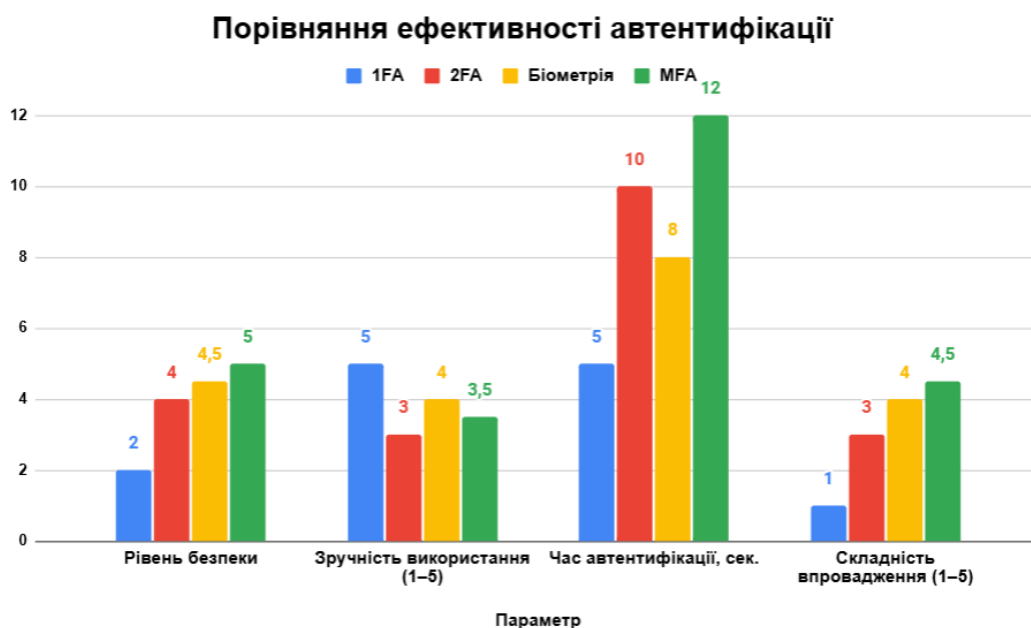


Рисунок 4.2 – Графік порівняння ефективності автентифікації

MFA забезпечує найвищий рівень захищеності, що робить її пріоритетним вибором для середовищ із високим рівнем загроз. Попри зростання часу автентифікації, MFA забезпечує баланс між безпекою та зручністю. Висока складність впровадження і витрати на підтримку виправдані для корпоративних середовищ, але можуть бути надмірними для малих організацій. MFA є ідеальним вибором для критичних систем, де безпека має найвищий пріоритет. Для менш ризикових середовищ можуть бути доцільними дешевші методи, як 2FA.

4.3 Результати впровадження WPA3 та MFA в комплексі

У цьому підрозділі проаналізовано, як впровадження WPA3 у поєднанні з багатофакторною автентифікацією (MFA) допомагає боротися з найпоширенішими атаками на бездротові мережі. Оцінка базується на аналізі ефективності протидії основним типам атак, включаючи несанкціонований

доступ, атаки типу "людина посередині" (MitM), атаки на мережеве обладнання, DDoS, атаку KRACK та атаки на рівні автентифікації.

Основні цілі впровадження WPA3 та MFA:

- забезпечення захисту від атак грубої сили та підбору паролів;
- шифрування даних для запобігання перехоплення трафіку;
- введення багатофакторної автентифікації для перевірки користувачів на декількох рівнях;
- захист мережевого обладнання від несанкціонованих змін та зловмисного використання.

В таблиці 4.3 наведено результати ефективності WPA3 та MFA для протидії основним атакам.

Таблиця 4.3 - Рівень ефективності WPA3 та MFA для протидії основним атакам

Тип атаки	Вразливість без захисту (%)	WPA3 (%)	MFA (%)	WPA3+MFA (%)
Несанкціонований доступ	85%	40%	15%	5%
Атаки типу "людина посередині"	70%	20%	10%	5%
Атаки на мережеве обладнання	60%	30%	20%	10%
DDoS	50%	40%	15%	10%
Атака KRACK	80%	10%	0%	0%
Атаки на рівні автентифікації	75%	20%	5%	2%

На рисунку 4.3 зображено візуальне порівняння ефективності впровадження WPA3 та MFA для протидії основним атакам.

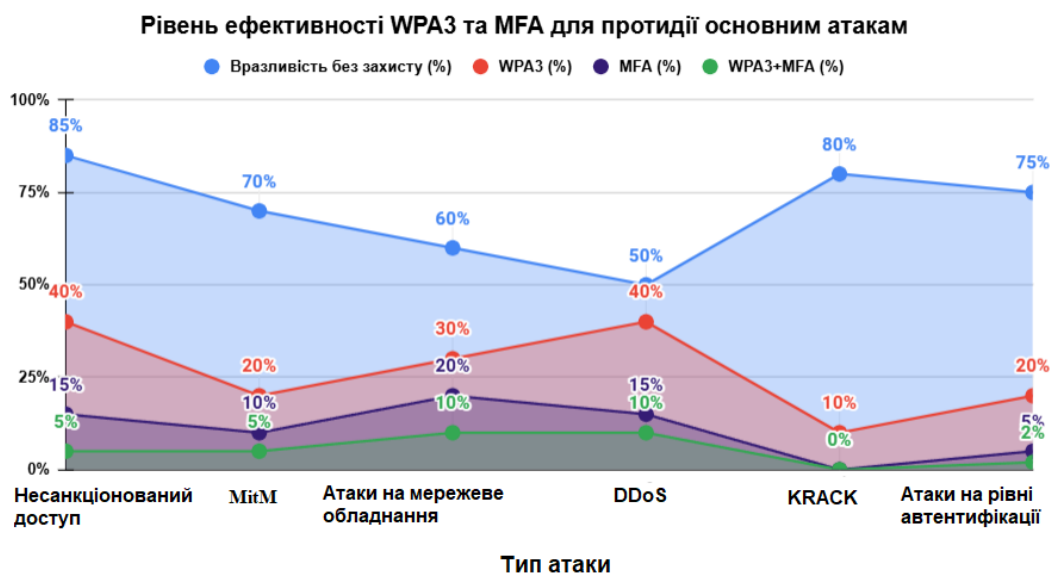


Рисунок 4.3 – Графік ефективності протидії основним атакам

Аналіз результатів:

- несанкціонований доступ: WPA3 значно підвищує безпеку завдяки протоколу SAE, який запобігає зламу навіть за умов слабких паролів. MFA додає додатковий рівень захисту, вимагаючи підтвердження особи через OTP або біометричні дані;
- MitM: завдяки Opportunistic Wireless Encryption (OWE) WPA3 шифрує навіть відкриті мережі, що знижує ризик перехоплення даних. MFA унеможливорює отримання доступу зловмисником навіть у разі перехоплення;
- DDoS: WPA3 оптимізує обробку трафіку, зменшуючи вразливість до перевантаження. MFA мінімізує можливість атак на рівні автентифікації;
- KRACK: WPA3 повністю усуває вразливості протоколу WPA2, захищаючи від перехоплення та повторного використання ключів.

В таблиці 4.4 можна побачити продуктивність мережі під час атак.

Таблиця 4.4 - Продуктивність мережі під час атак

Метод захисту	Швидкість завантаження (Mbps)	Швидкість відправлення (Mbps)	Втрати пакетів (%)	Час автентифікації (с)
Без захисту	40	38	10%	1.0

Продовження таблиці 4.4

Метод захисту	Швидкість завантаження (Mbps)	Швидкість відправлення (Mbps)	Втрати пакетів (%)	Час автентифікації (с)
WPA2	90	85	1.8%	2.0
WPA3	88	84	0.5%	2.2
WPA3+MFA	85	82	0.2%	3.5

Приклад сценарію атаки та ефективність захисту:

- сценарій: зловмисник здійснює атаку типу "людина посередині" у відкритій мережі;
- дії WPA3: усі з'єднання зашифровані завдяки OWE, що унеможлиблює перехоплення трафіку;
- дії MFA: навіть у разі компрометації трафіку зловмисник не може пройти автентифікацію через вимогу OTP або біометрії;
- результат: атака блокується, а користувач залишається захищеним.

WPA3 забезпечує сучасний рівень захисту від основних атак, таких як перехоплення даних, DDoS та атака KRACK. MFA додає додатковий рівень перевірки, що суттєво ускладнює злом навіть при компрометації базових облікових даних. У поєднанні WPA3 та MFA забезпечують мінімальний рівень вразливості до будь-яких атак, роблячи бездротові мережі максимально захищеними. Рекомендовано використовувати ці методи разом у середовищах із високими вимогами до безпеки, особливо у корпоративних мережах.

ВИСНОВКИ

У цій дипломній роботі детально досліджено актуальну проблему безпеки бездротових мереж та запропоновано ефективне рішення для її подолання шляхом впровадження багатофакторної автентифікації (MFA) та сучасних стандартів шифрування, таких як WPA3. З розвитком бездротових технологій кількість підключених пристроїв стрімко зростає, що спричиняє підвищення ризику кібератак і вразливостей. Мета роботи полягала в впровадженні комплексної системи захисту, яка забезпечить високий рівень безпеки переданих даних у бездротових мережах та відповідатиме сучасним вимогам кібербезпеки.

У процесі роботи проведено ґрунтовний аналіз основних загроз і вразливостей бездротових мереж. Зокрема, розглянуто такі типи атак, як несанкціонований доступ, атаки типу "людина посередині" (Man-in-the-Middle), DDoS-атаки, атака KRACK та загрози, пов'язані з недостатньою безпекою автентифікації. Кожна з цих загроз несе суттєві ризики, особливо в умовах активного використання мереж для передачі конфіденційної інформації. Застарілі стандарти шифрування, такі як WEP, та недостатній рівень автентифікації користувачів є ключовими факторами, що сприяють успішному виконанню атак.

У роботі проведено порівняльний аналіз існуючих стандартів шифрування, таких як WEP, WPA, WPA2 та WPA3. Визначено, що WPA3 є найбільш сучасним та ефективним стандартом, який відповідає сучасним викликам у сфері кібербезпеки. Використання WPA3 дозволяє забезпечити стійкість до атак типу brute force завдяки впровадженню алгоритму Simultaneous Authentication of Equals (SAE) та унікальності ключів для кожної сесії. Крім того, WPA3 гарантує конфіденційність навіть у відкритих мережах завдяки шифруванню Opportunistic Wireless Encryption (OWE).

Впровадження системи багатофакторної автентифікації, яка включає два рівні перевірки користувачів: введення пароля та використання одноразового

пароля (OTP). Перший рівень передбачає перевірку облікових даних користувача в базі даних сервером автентифікації. У разі успішного введення пароля користувач переходить до другого рівня, а саме введення OTP. OTP надається користувачу через мобільний додаток, наприклад, Google Authenticator. Такий підхід значно ускладнює несанкціонований доступ до мережі та робить систему стійкою до спроб злому.

У роботі також розглянуто можливість інтеграції запропонованої системи з існуючими бездротовими мережами. Це включає налаштування WPA3 для захисту з'єднань, впровадження алгоритмів генерації OTP та створення надійної бази даних користувачів. Продемонстровано, що система легко адаптується до різних сценаріїв використання, забезпечуючи безперебійну роботу мережі.

У процесі тестування запропонованої системи проводилися вимірювання її ефективності за різними параметрами, такими як швидкість передачі даних, затримка, втрати пакетів та стійкість до атак. Результати показали, що впровадження WPA3 у поєднанні з MFA забезпечує максимальний рівень безпеки без суттєвого впливу на продуктивність мережі. У порівнянні з попередніми стандартами, такими як WPA2, система продемонструвала значне зниження вразливостей до сучасних атак.

Впроваджена система може бути реалізована в організаціях, які працюють із конфіденційними даними. Крім того, пропоновані рішення можуть бути використані у побутових умовах для підвищення безпеки домашніх бездротових мереж.

Отже, виконана робота демонструє, що сучасні стандарти шифрування, зокрема WPA3, у поєднанні з багатофакторною автентифікацією є ефективним інструментом для забезпечення захисту бездротових мереж. Це дозволяє значно знизити ризики кібератак, підвищити рівень безпеки переданих даних та створити надійну інфраструктуру для подальшого розвитку технологій бездротового зв'язку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Ahson S., Ilyas M. WiMAX: standards and security. Taylor & Francis Group, 2018. 276 p.
2. Bawany, N.Z., Shamsi, J.A. & Salah, K. DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. Arab J Sci Eng 42, 425–441 (2017). <https://doi.org/10.1007/s13369-017-2414-5> (дата звернення: 29.09.2024).
3. Chen L., Ji J., Zhang Z. Wireless network security. Berlin, Heidelberg : Springer Berlin Heidelberg, 2013. URL: <https://doi.org/10.1007/978-3-642-36511-9> (date of access: 14.10.2024).
4. Chen M., Gündüz D., Huang K. Distributed learning in wireless networks: recent progress and future challenges. IEEE journal on selected areas in communications. 2021. Vol. 39, no. 12. P. 3579–3605. URL: <https://doi.org/10.1109/JSAC.2021.3118346> (date of access: 02.10.2024).
5. Demystifying internet of things security / S. Cheruvu et al. Berkeley, CA : Apress, 2020. URL: <https://doi.org/10.1007/978-1-4842-2896-8> (date of access: 14.10.2024).
6. Gunasekaran N., Redd S. Bluetooth in wireless communication. IEEE communications magazine. 2002. Vol. 40, no. 6. P. 90–96. URL: <https://doi.org/10.1109/MCOM.2002.1007414> (date of access: 03.10.2024).
7. Kanade A., Ranganathan C., Ramachandran G. Analysis of wireless network security in internet of things and its applications. Engineering. 2024. Vol. 21, no. 55. P. 1–12. URL: <https://doi.org/10.54905/disssi.v21i55.e1ije1675> (date of access: 24.09.2024).
8. Mughal A. A. Well-Architected wireless network security. Journal of humanities and applied science research. 2022. Vol. 5, no. 1. P. 32–42. URL: <https://journals.sagescience.org/index.php/JHASR/article/view/52> (date of access: 23.09.2024).

9. Network and system security / ed. by J. K. Liu, X. Huang. Cham : Springer International Publishing, 2019. URL: <https://doi.org/10.1007/978-3-030-36938-5> (date of access: 14.10.2024).
10. Osterhage W. Wireless network security. Taylor & Francis Group, 2021.
11. Patras P., Zhang C. Deep learning in mobile and wireless networking: a survey. IEEE communications surveys & tutorials. 2019. Vol. 21, no. 3. P. 2224–2287. URL: <https://doi.org/10.1109/COMST.2019.2904897> (date of access: 03.10.2024).
12. Shin M., Ma J., Arbaugh W. Wireless network security and interworking. Proceedings of the IEEE. 2006. Vol. 94, no. 2. P. 455–466. URL: <https://doi.org/10.1109/JPROC.2005.862322> (date of access: 26.09.2024).
13. Wifi networking book : WLAN standards: IEEE 802. 11 bgn, 802. 11n, 802. 11ac and 802. 11ax. Independently Published, 2019.
14. Zhu F., Zhang C., Farouk A. Practical network coding technologies and softwarization in wireless networks. IEEE internet of things journal. 2021. Vol. 8, no. 7. P. 5211–5218. URL: <https://doi.org/10.1109/JIOT.2021.3056580> (date of access: 01.10.2024).
15. Брюхов Б.Р., Киричек Г.Г. Багатофакторна автентифікація та шифрування в бездротових мережах. Матеріали XII міжнародної науко-во-практичної конференції «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій», 10-12 грудня 2024 року, Запоріжжя. 2024
16. Брюхов Б., Тягунова М., Створення ефективної комп'ютерної мережі для лікарні. Технологія-2024 : Матеріали XXVII міжнар. науково-техн. конф., м. Київ, 24 трав. 2024 р. Київ, 2023. С. 180.
17. Гальчинський, Л. Ю., & Корольова, В. Р. (2024). Оцінка захищеності бездротових мереж у міському середовищі з урахуванням використання протоколів безпеки. Інфокомунікаційні та комп'ютерні технології, 2(06), 9-21. <https://doi.org/10.36994/2788-5518-2023-02-06-01> (date of access: 27.09.2024).

18. Козел В. Класифікація та рекомендації захисту від МІТМ атак. Проблеми інформаційних технологій. 2019. Т. 25, № 1. С. 58–65. URL: <http://eir.kntu.net.ua/jspui/handle/123456789/517>.

19. Крівенко С., Ротаньова Н., Лазаревська Ю. Дослідження системи на уразливість до мітм атаки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2021. Т. 1, № 13. С. 29–38. URL: <https://doi.org/10.28925/2663-4023.2021.13.2938> (дата звернення: 30.09.2024).

20. Переверзєв А., Левченко С., Ніколаєвський О. Новітні протоколи бездротових мереж: переваги та недоліки. Вісник Хмельницького національного університету. Серія: технічні науки. 2024. Т. 335, № 3. С. 445–449. URL: <https://doi.org/10.31891/2307-5732-2024-335-3-61> (дата звернення: 05.10.2024).

21. Скидан Д., Гальчинський Л. Оцінка рівня захищеності протоколів безпеки для бездротових мереж. Collection of scientific papers «SCIENTIA». 2024. Т. 15, № 2. С. 113–117. URL: <https://previous.scientia.report/index.php/archive/article/view/1893> (дата звернення: 26.09.2024).

22. Хмельницький О., Хмельницький Ю. Цілісність та конфіденційність передачі даних у мережах. Вимірювальна та обчислювальна техніка в технологічних процесах. 2013. № 1. С. 214–217. URL: <https://elar.khmnu.edu.ua/handle/123456789/2155> (дата звернення: 30.09.2024).