

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»



Факультет комп'ютерних наук та технологій
Кафедра «Комп'ютерні системи та мережі»

БРЮХОВ БОГДАН РУСЛАНОВИЧ
Група КНТ-513м

СИСТЕМА ЗАХИСТУ БЕЗДРотових МЕРЕЖ ІЗ
ВИКОРИСТАННЯМ БАГАТОФАКТОРНОЇ
АВТЕНТИФІКАЦІЇ

АВТОРЕФЕРАТ

магістерської роботи на здобуття освітньо-кваліфікаційного
рівня «магістр» 123 «Комп'ютерна інженерія»
освітньої програми «Комп'ютерні системи та мережі»

2024 р.

Магістерська робота є рукопис.

Робота виконана в Національному університеті «Запорізька політехніка», на кафедрі комп'ютерних систем та мереж

Керівник

кандидат технічних наук, доцент
Киричек Галина Григорівна,
Національний університет «Запорізька
політехніка», доцент кафедри
комп'ютерних систем та мереж

**Офіційний
рецензент:**

доктор технічних наук, доцент
Єфименко Микола Володимирович,
Національний університет «Запорізька
політехніка», професор кафедри
комп'ютерних систем та мереж

Захист відбудеться "13" грудня 2024 р.

Секретар екзаменаційної комісії, доцент кафедри
комп'ютерних систем та мереж **Т.В. Голуб**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. 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.

Мета і завдання дослідження. Мета магістерської роботи полягає у дослідженні та забезпеченні безпеки бездротових мереж шляхом впровадження системи захисту, яка поєднає сучасні методи шифрування та багатофакторну автентифікацію.

Для досягнення поставленої мети необхідно виконати такі основні завдання:

1. 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;

2. 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;

3. Впровадження моделі захисту бездротових мереж: побудова моделі, що включає шифрування даних та багатофакторну автентифікацію для забезпечення надійного захисту користувачів і мережі;

4. Впровадження шифрування даних: вибір та інтеграція надійних методів шифрування для захисту переданої інформації у бездротовій мережі;

5. Реалізація механізмів багатофакторної автентифікації: проєктування механізмів автентифікації, що включають кілька рівнів перевірки ідентичності користувачів, таких як паролі, біометричні дані, смс-коди або апаратні токени;

6. Аналіз ефективності впроваджених методів: проведення порівняння впровадженої системи з іншими методами захисту мережі для оцінки її ефективності у різних сценаріях використання та умовах експлуатації.

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

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

Методи дослідження базуються на аналізі сучасних стандартів бездротових мереж, вивченні їх уразливостей і ефективності захисту, моделюванні системи захисту із використанням багатофакторної автентифікації.

Наукова новизна отриманих результатів:

Впроваджено систему захисту бездротових мереж, яка поєднує сучасний стандарт шифрування WPA3 та багатофакторну автентифікацію. Модель забезпечує підвищений рівень безпеки за

рахунок зменшення кількості вразливостей, зберігаючи продуктивність мережі.

Практичне значення отриманих результатів:

Впровадження розробленої системи захисту бездротових мереж дозволяє значно підвищити рівень безпеки передачі даних, знизити ризик несанкціонованого доступу та захистити інформацію від сучасних кіберзагроз.

Апробація результатів магістерської роботи. Основні положення магістерської роботи та результати досліджень подано до участі на конференції:

– 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.

– 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.

Структура та обсяг роботи. Магістерська робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел. Основна частина містить 68 сторінок, 21 рисунок і 8 таблиць, список використаних джерел зі 22 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У першому розділі проведено аналіз розглянуто основні поняття бездротових мереж, їх типи та класифікацію. Основна увага приділена мережам Wi-Fi як найбільш розповсюджені варіанту для передачі даних. Проведено огляд класифікації бездротових мереж та аналіз стандартів сімейства IEEE 802.11, який є один із найпоширеніших стандартів для бездротових мереж, відомий завдяки популярним Wi-Fi технологіям. На основі огляду зроблено висновки щодо важливості Wi-Fi для створення високошвидкісного підключення, що поєднує зручність та мобільність.

В результаті аналізу приведено модель захисту бездротових мереж вона представлена на рисунку 1, яка забезпечує підвищену

безпеку користувачів завдяки використанню багатофакторної автентифікації та системи шифрування даних.

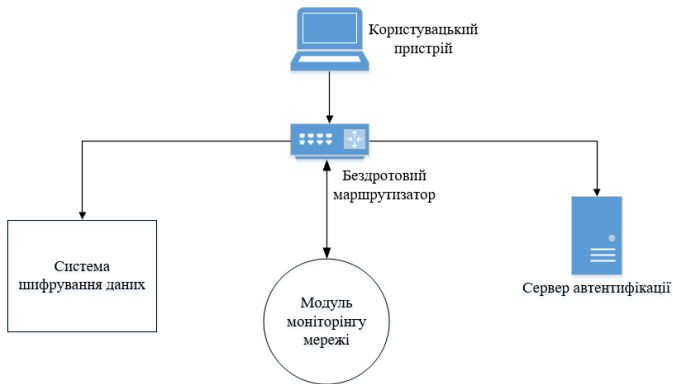


Рисунок 1 – Модель захисту

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

У **другому розділі** увагу присвячено аналізу безпеки та технологій захисту бездротових мереж. У ньому розглянуто основні загрози, пов'язані із захистом бездротових мереж, такі як DDoS, атаки типу "людина посередині" (MitM), злом мережевого обладнання, KRACK-атаки та брутфорс.

Проведено детальний огляд методів шифрування, зокрема стандартів WEP, WPA, WPA2, та WPA3, їх вразливостей і переваг. Акцент зроблено на оптимальних підходах до захисту, які враховують сучасні вимоги до безпеки, зокрема багатофакторну автентифікацію та шифрування WPA3.

Розділ також містить аналіз ефективності методів захисту з точки зору протидії основним загрозам та забезпечення безперебійної роботи бездротових мереж.

У **третьому розділі** детально описано впровадження системи захисту бездротових мереж, що базується на використанні

сучасного стандарту шифрування WPA3 та багатофакторної автентифікації (MFA). Схема зображена на рисунку 2.

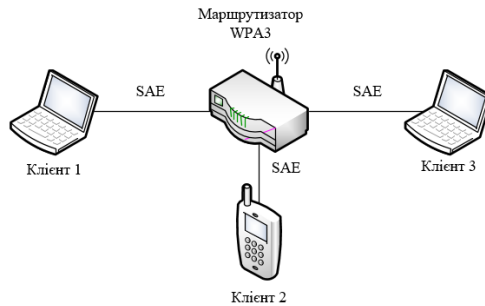


Рисунок 2 – Схема налаштування WPA3 у бездротовій мережі

Висвітлено процес реалізації WPA3. Розглянуто налаштування точок доступу та клієнтських пристроїв, перевірено сумісність із сучасним мережевим обладнанням. Описано переваги WPA3, такі як захист від атак перебору пароля (brute force), Forward Secrecy та використання протоколу SAE. На рисунках 3 та 4 можна побачити впровадження WPA3.

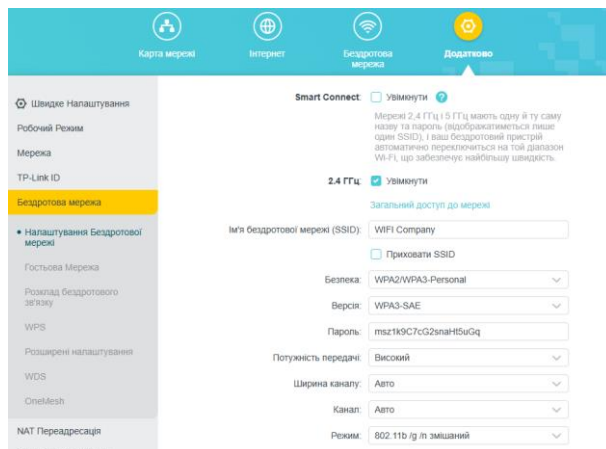


Рисунок 3 – Процес налаштування роутера

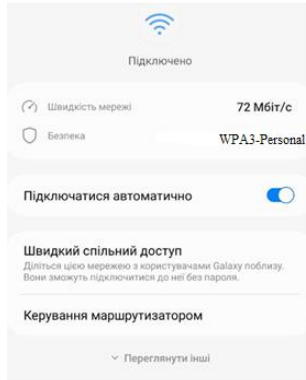


Рисунок 4 – Перевірка налаштування на пристрої

Також, присвячено реалізації механізмів багатофакторної автентифікації. У ньому наведено опис рівнів автентифікації (пароль, одноразові коди), особливості їх впровадження та функціонування.

Розглянуто інтеграцію MFA. Розділ також містить схеми, які демонструють архітектуру системи та взаємодію її компонентів. Така система базується на поєднанні різних факторів автентифікації: знань та володіння. Описано структуру системи, принципи її функціонування та сумісність із бездротовими мережами. Система автентифікації з кількома рівнями перевірки складається з різних компонентів, які можна побачити на рисунку 5.

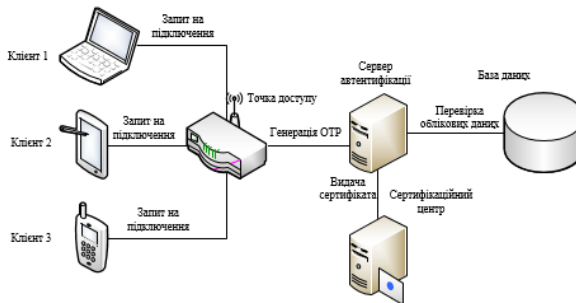


Рисунок 5 – Схема багатофакторної автентифікації

Описано створення системи та її реалізація. Запропонований алгоритм процесу роботи багатofакторної автентифікації. На початку зустрічає вітальна сторінка, на якій є кнопка за допомогою якої можна перейти до першого рівня автентифікації рисунок 6.

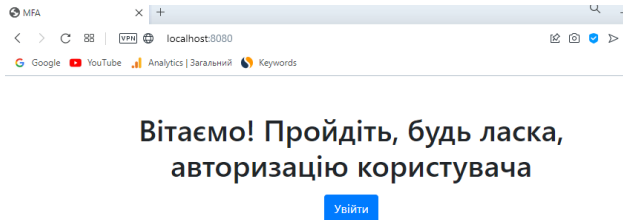


Рисунок 6 – Перша сторінка, яка зустрічає користувача

Перший рівень (пароль) (рис. 7):

- 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 введено невірно то виводиться повідомлення про помилку

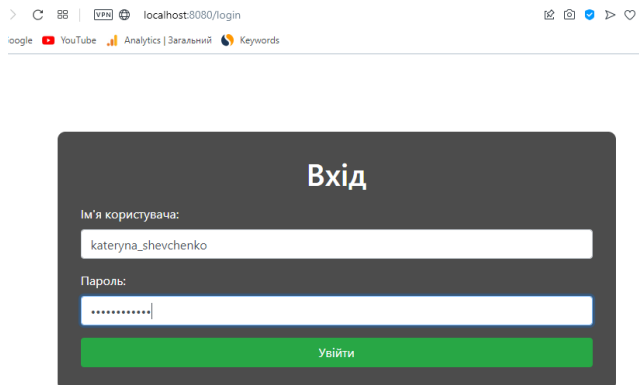


Рисунок 7 – Перший рівень автентифікації (пароль)

Другий рівень (одноразовий пароль) (рис. 8-10):

- після успішного проходження першого рівня, користувач може побачити сторінку на якій буде зображено QR-код. Після сканування переходить на наступну сторінку;
- сервер автентифікації генерує OTP за алгоритмом TOTP (Time-based One-Time Password);
- користувач вводить OTP 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;
- авторизація користувача при правильному вводі коду.

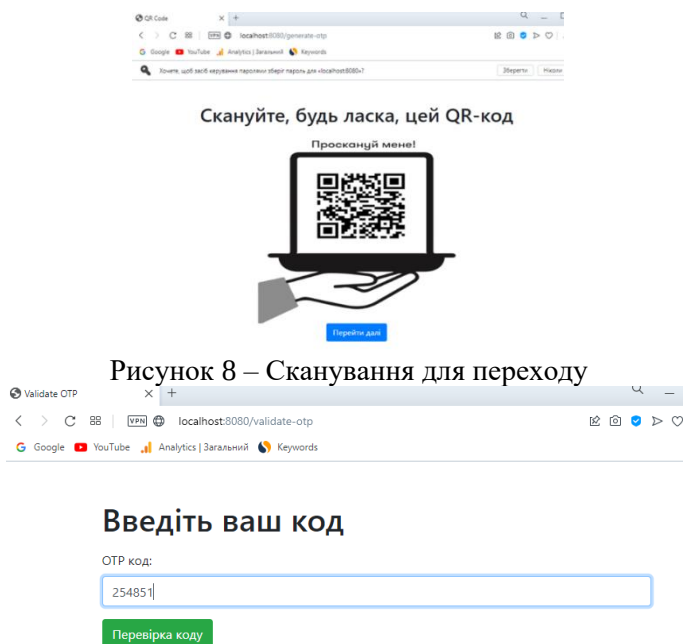


Рисунок 9 – Другий рівень автентифікації (OTP)

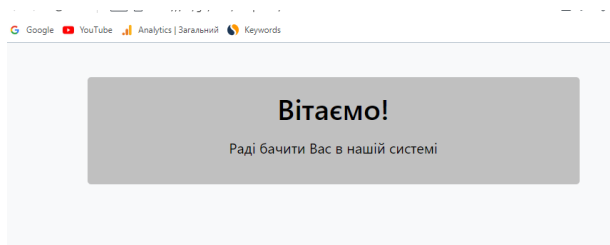


Рисунок 10 – Результат введення вірного коду (ОТР)

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

У **четвертому розділі** присвячено аналізу ефективності впроваджених методів захисту бездротових мереж, таких як WPA3 і багатofакторна автентифікація (MFA). результати оцінки WPA3 як сучасного стандарту шифрування. Проведено тестування його ефективності порівняно з попередніми стандартами (WEP, WPA, WPA2) за такими показниками: рівень безпеки, швидкість передачі даних, затримка і стійкість до атак. Показано на рисунку 11, що WPA3 забезпечує суттєве підвищення захисту завдяки використанню сучасних криптографічних алгоритмів.

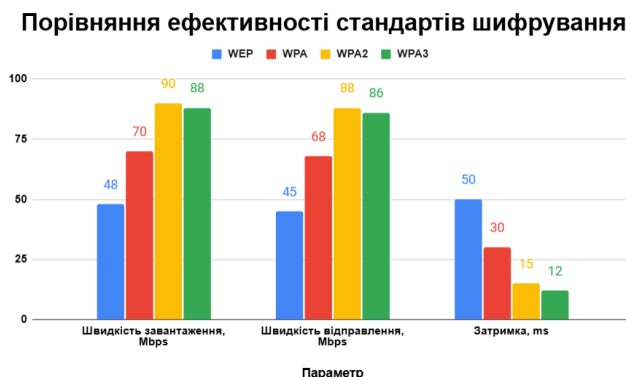


Рисунок 11 – Порівняння ефективності стандартів шифрування

Аналіз впровадження MFA та порівнює її з альтернативними методами автентифікації: однофакторною (1FA), двофакторною

(2FA) і біометричною автентифікацією. Результати представлено у вигляді таблиць, що демонструють підвищення рівня захисту та доступності при використанні MFA.

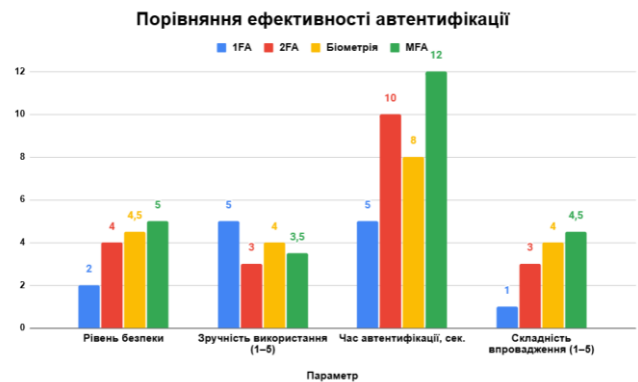


Рисунок 12 – Графік порівняння ефективності автентифікації

Проведено оцінку роботи WPA3 та MFA в комплексі. Аналіз включає тестування системи за різних сценаріїв атак (DDoS, MitM, KRACK). Графіки ілюструють ефективність комбінованого підходу, який забезпечує найвищий рівень захисту та мінімізує ризики.

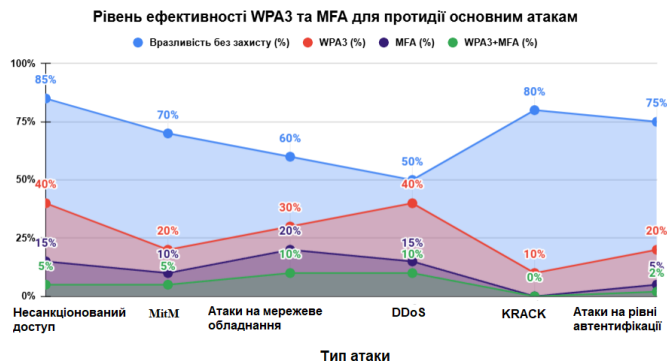


Рисунок 13 – Графік ефективності протидії основним атакам

Результати дослідження підтверджують, що впроваджена система значно підвищує рівень безпеки бездротових мереж і є придатною для застосування в сучасних інформаційних інфраструктурах.

ВИСНОВКИ

У роботі проведено комплексний аналіз та впровадження системи захисту бездротових мереж на основі сучасних стандартів WPA3 та багатофакторної автентифікації (MFA). Здійснено оцінку ефективності впровадження системи для протидії основним загрозам, включаючи атаки типу "людина посередині", DDoS, KRACK та злом автентифікації.

Основні результати дослідження:

1. Впровадження WPA3: забезпечує високий рівень шифрування даних, захист від атак грубої сили та підвищену стійкість до перехоплення трафіку. Усуває вразливості попередніх стандартів, таких як WPA2.
2. Інтеграція MFA: надано декілька рівнів перевірки користувача: паролі, одноразові коди. Доведено, що MFA значно знижує ризик несанкціонованого доступу навіть у випадку компрометації одного з факторів.
3. Результати поєднання WPA3 та MFA забезпечує найвищий рівень захисту серед протестованих систем та зменшує кількість вразливостей.

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.