Міністерство освіти і науки України
Український державний університет науки і технологій

Комп'ютерних технологій і систем
(назва факультету)

Електронні обчислювальні машини
(повна назва кафедри)

До захисту
19.01.2024

Пояснювальна записка
до кваліфікаційної роботи
магістра
(ступінь вищої освіти)

на тему: Комплексна тема «Розробка комплексу лабораторних робіт щодо дослідження бездротової мережі WI-Fi». Дослідження механізмів безпеки бездротової мережі Wi-Fi

за освітньою програмою Комп'ютерна інженерія
зі спеціальності: 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

Виконав: студент групи: КС2221

(підпис студента) / Владислав КОМПАНІЄЦЬ /
(Ім'я ПРІЗВИЩЕ)

Керівник: (підпис) /проф. Ігор ЖУКОВИЦЬКИЙ/
(посада, Ім'я ПРІЗВИЩЕ)

Нормоконтролер: (підпис) /доц. Володимир ШАПОВАЛОВ/
(посада, Ім'я ПРІЗВИЩЕ)

Засвідчую, що у цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент (підпис)

Дніпро – 2024 рік

Ministry of Education and Science of Ukraine
Ukrainian State University of Science and Technologies

Computer Technologies and Systems
(faculty)

Electronic Computers
(department)

Explanatory Note
to Master's Thesis
(higher education degree)

on the topic: Comprehensive topic: «Development of a set of laboratory works for the investigation of a Wi-Fi wireless network». Section: «Study of Wi-Fi wireless network security mechanisms»

according to educational curriculum Computer Engineering

in the Speciality: 123 Computer Engineering
(speciality and its code)

Done by the student of the group: КС2221 / Vladyslav Kompaniiets /
(name, surname)

Scientific Supervisor: / Igor Zhukovytskyy /
(position, name, surname)

Normative controller : / Oleksandr Shapovalov /
(position, name, surname)

Dnipro – 2024

Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет: Комп'ютерні технології і системи
Кафедра: Електронні обчислювальні системи
Рівень вищої освіти: Другий (магістерський)
Освітня програма: Комп'ютерна інженерія
Спеціальність: 123 Комп'ютерна інженерія
(шифр та назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри ЕОМ
(підпис) Ігор ЖУКОВИЦЬКИЙ
(Ім'я ПРІЗВИЩЕ)
Дата 15.11.2023

З А В Д А Н Н Я

на кваліфікаційну роботу магістра
(ступінь вищої освіти)

студенту Компанійцю Владиславу Вадимовичу
(Прізвище, Ім'я По батькові)

1. Тема роботи: Комплексна тема «Розробка комплексу лабораторних робіт щодо дослідження бездротової мережі WI-Fi». Розділ «Дослідження механізмів безпеки бездротової мережі Wi-Fi»

Керівник роботи: Жуковицький Ігор Володимирович
(Прізвище, Ім'я, По батькові, науковий ступінь, вчене звання)

затверджені наказом від "10" жовтня 2023 р. № 1005ст

2. Строк подання студентом роботи: 23.01.2024 р.
3. Вихідні дані до роботи: Технічний опис мережі Wi-Fi, опис обладнання мережевих лабораторій кафедри ЕОМ.
4. Зміст пояснювальної записки (перелік питань, які потрібно опрацювати):
4.1. Аналіз основних принципів захисту бездротової мережі Wi-Fi та засобів навчання студентів цих принципам.
4.2. Принципи налагодження можливих механізмів захисту бездротової мережі Wi-Fi на обладнанні лабораторій кафедри ЕОМ.
4.3. Дослідження роботи механізмів захисту бездротової мережі Wi-Fi.
4.4. Розробка лабораторних робіт та контрольних запитань щодо заданої тематики.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Вступ	09.10.2023	5%
2	Аналіз основних принципів захисту бездротової мережі Wi-Fi та засобів навчання студентів цих принципам.	03.11.2023	20%
3	Принципи налагодження можливих механізмів захисту бездротової мережі Wi-Fi на обладнанні лабораторій кафедри ЕОМ.	23.11.2023	20%
4	Дослідження роботи механізмів захисту бездротової мережі Wi-Fi.	10.12.2023	25%
5	Розробка лабораторних робіт та контрольних запитань щодо заданої тематики.	26.12.2023	25%
6	Висновки	11.01.2024	5%
7	Подання кваліфікаційної роботи до кафедри	15.01.2024	
8	Захист кваліфікаційної роботи на засіданні Екзаменаційної комісії	23.01.2024	

Студент _____ (підпис) Владислав КОМПАНІЄЦЬ (Ім'я ПРІЗВИЩЕ)

Керівник роботи _____ (підпис) Ігор ЖУКОВИЦЬКИЙ (Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи магістра:

84 с., 33 рис., 4 табл., 19 джерел.

Об'єкт дослідження – безпека бездротових мереж Wi-Fi.

Предмет дослідження – механізми захисту бездротових мереж Wi-Fi від несанкціонованого доступу та перехоплення трафіку.

Мета роботи – розробка комплексу лабораторних робіт для дослідження механізмів безпеки бездротових мереж Wi-Fi студентами кафедри ЕОМ.

Методи дослідження – аналіз науково-технічної літератури, експериментальні дослідження безпеки Wi-Fi мережі з використанням Wireshark та Aircrack-ng, статистична обробка результатів.

Одержані результати – у роботі проаналізовано стандарти безпеки бездротових мереж, досліджено методи налаштування механізмів захисту Wi-Fi. Проведено експериментальні дослідження щодо перехоплення трафіку у тестовій мережі. Розроблено 2 лабораторні роботи для вивчення студентами питань забезпечення безпеки бездротового зв’язку.

Ключові слова: БЕЗПЕКА, WI-FI, WIRESHARK, AIRCRACK-NG, ЛАБОРАТОРНА РОБОТА.

ЗМІСТ

ВСТУП ТА ПОСТАНОВКА ЗАВДАННЯ

Бездротові мережі Wi-Fi набули широкого поширення в останні роки. Вони використовуються в офісах, навчальних закладах, громадських місцях. Однак питання забезпечення безпеки Wi-Fi мереж залишається гострою проблемою. Адже перехоплення трафіку може призвести до крадіжки конфіденційних даних та порушення приватності. Тому підготовка фахівців з кібербезпеки, здатних захистити Wi-Fi мережі, є вкрай актуальною.

Мета і завдання дослідження. Метою роботи є розробка комплексу лабораторних робіт для дослідження механізмів безпеки бездротових мереж Wi-Fi студентами кафедри ЕОМ.

Завдання:

- проаналізувати принципи захисту Wi-Fi та методи навчання;
- дослідити налаштування захисту на обладнанні лабораторій;
- провести дослідження механізмів захисту Wi-Fi;
- розробити лабораторні роботи та тести.

Об’єкт дослідження – безпека бездротових мереж Wi-Fi.

Предмет – механізми захисту Wi-Fi від перехоплення трафіку.

Методи та засоби дослідження – аналіз літератури, експериментальні дослідження з використанням Wireshark та Aircrack-ng, статистична обробка результатів.

Наукова новизна полягає у розробці комплексу лабораторних робіт для вивчення безпеки Wi-Fi.

Структура роботи: вступ, 4 розділи, висновки, список використаних джерел.

Розділ 1 - аналіз принципів захисту Wi-Fi та методів навчання. Розділ 2 - налаштування захисту Wi-Fi. Розділ 3 - дослідження механізмів захисту. Розділ 4 - розробка лабораторних робіт та тестів.

Матеріали магістерської роботи опубліковані в тезах конференцій (додатки В, Г). [3,4]

1 АНАЛІЗ ОСНОВНИХ ПРИНЦИПІВ ЗАХИСТУ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI ТА ЗАСОБІВ НАВЧАННЯ СТУДЕНТІВ ЦИМ ПРИНЦИПАМ

1.1 Базові принципи роботи Wi-Fi

1.1.1 Визначення та коротка історія бездротових мереж Wi-Fi

Wi-Fi (скорочено від «Wireless Fidelity») є технологією, що дозволяє електронним пристроям підключатися до мережі через радіохвилі без використання дротових з'єднань. Це особливо корисно для мобільних пристроїв, таких як смартфони, планшети та ноутбуки, але також використовується у стаціонарних комп'ютерах, телевізорах, принтерах та інших пристроях.

Спектри застосування Wi-Fi надзвичайно широкі. Від домашніх мереж, де користувачі підключають свої пристрої до Інтернету, до публічних мереж у кафе, готелях, аеропортах та інших громадських місцях. Корпорації використовують Wi-Fi для підключення працівників, а міста розгортають муніципальні мережі Wi-Fi для забезпечення доступу до Інтернету своїм громадянам. [2]

Історія Wi-Fi почалася в 1970-х, коли перші експерименти з бездротовими мережами були проведені. Проте саме поняття "Wi-Fi" з'явилось лише в кінці 1990-х, завдяки співпраці кількох компаній, які мали за мету створити стандарт для бездротового підключення. У 1997 році було запропоновано перший стандарт, відомий як IEEE 802.11. Цей стандарт мав обмежену швидкість передачі даних, але він став основою для подальшого розвитку технології.

З того часу Wi-Fi пройшла довгий шлях розвитку. З'явились нові стандарти, які збільшили швидкість передачі даних, покращили безпеку та розширили можливості застосування. Сьогодні Wi-Fi можна знайти майже в будь-якому побутовому пристрої, від смартфонів до холодильників, і вона продовжує розвиватися, надаючи користувачам все більше можливостей для бездротового підключення.

1.1.2 Стандарти Wi-Fi

Wi-Fi включає в себе кілька стандартів, розроблених комітетом IEEE 802.11. Ці стандарти визначають характеристики різних типів бездротових мереж, включаючи частотні діапазони, швидкості передачі даних та інші технічні особливості. На рисунку 1.1 проілюстровано історію розвитку стандарту IEEE 802.11. [1]

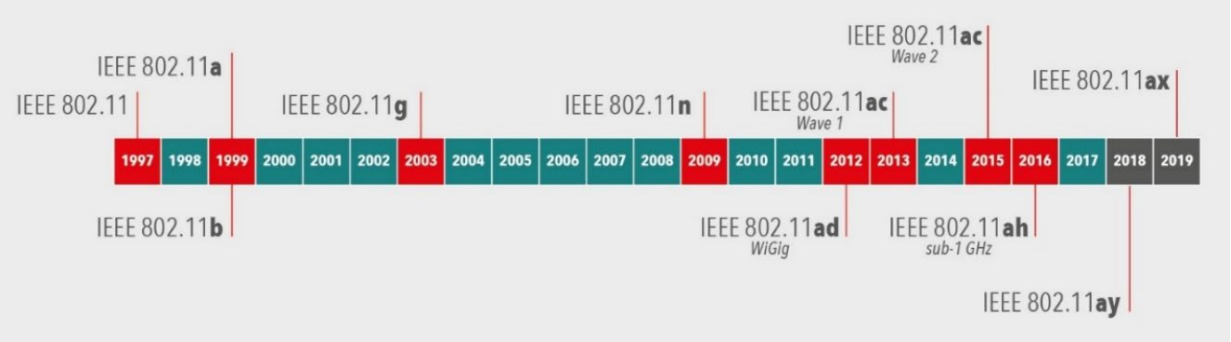

Рисунок 1.1 – Розвиток стандарту IEEE 802.11

а) **IEEE 802.11a (1999 р.)**: Використовує частотний діапазон 5 GHz та забезпечує швидкість передачі даних до 54 Mbps. Цей стандарт став популярним у бізнес-середовищі завдяки високій швидкості та меншому завадам порівняно з 2,4 GHz.

б) **IEEE 802.11b (1999 р.)**: Робочий діапазон 2,4 GHz, з максимальною швидкістю 11 Mbps. Став першим широко розповсюдженим стандартом Wi-Fi у домашніх та офісних мережах.

в) **IEEE 802.11g (2003 р.)**: Також працює на 2,4 GHz, але надає швидкості до 54 Mbps. Сумісний зі стандартом 802.11b.

г) **IEEE 802.11n (2009 р.)**: Введення технології MIMO (Multiple Input, Multiple Output), що дозволило збільшити швидкість передачі даних до 600 Mbps. Підтримує обидва частотних діапазони: 2,4 GHz та 5 GHz.

д) **IEEE 802.11ac (2013 р.)**: Виключно на частоті 5 GHz, з максимальною швидкістю передачі даних 1 Gbps. Використовує удосконалену технологію MIMO та ширші канали для передачі даних.

е) **IEEE 802.11ax (2019 р.)**: Відомий як Wi-Fi 6, цей стандарт працює на обох частотних діапазонах і призначений для підтримки великої кількості пристроїв у високо завантажених мережах, надаючи швидкості до 10 Gbps.

Кожен наступний стандарт вносив покращення у швидкість, надійність та безпеку бездротового з'єднання. Сьогодні різні стандарти Wi-Fi можуть співіснувати в одній мережі, адаптуючись до потреб користувачів та особливостей обладнання.

В таблиці 1.1 відображено актуальні стандарти IEEE 802.11 на сьогоднішній день. [5]

Таблиця 1.1 Актуальні стандарти IEEE 802.11

Назва	Швидкість передачі	Частотний діапазон
802.11 n → Wi-Fi 4	600 Мбіт/с	2,4-2,5 або 5 ГГц
802.11 ac → Wi-Fi 5	від 433 Мбіт/с до 6,77 Гбіт/с	5 ГГц
802.11 ax → Wi-Fi 6	до 10747 Мбіт/с	від 1 ГГц до 5 ГГц

1.1.3 Фізичний рівень

Фізичний рівень бездротової мережі Wi-Fi відповідає за передачу даних між пристроями та мережею, визначаючи характеристики радіохвиль, які використовуються для комунікації. Поширені частоти для Wi-Fi – це 2,4 ГГц та 5 ГГц. Частота 2,4 ГГц має переваги у проникненні крізь перешкоди, але може зазнавати завад від інших пристроїв. З іншого боку, 5 ГГц забезпечує швидшу передачу даних з меншими завадами, але з меншим радіусом дії. [1]

Wi-Fi використовує різні методи модуляції для передачі даних, де однією з ключових технік є квадратурна амплітудна модуляція (QAM). Так, стандарт 802.11n може використовувати 64-QAM для оптимальної передачі. Також особливо важливою є технологія розширеного спектру OFDM, яка ділить сигнал на декілька вузьких частотних каналів для підвищення надійності передачі. [11]

Ширина каналу в Wi-Fi може коливатись від 20 МГц до 160 МГц. Хоча ширший канал може передавати більше даних, він також може бути більш

уразливим до завад. Додатково, міцність сигналу впливає на якість комунікації, залежно від відстані між пристроями, наявних перешкод та завад. Правильне розміщення та налаштування антен є ключовими для оптимізації міцності сигналу.

1.2 Принципи захисту бездротової мережі Wi-Fi

1.2.1 Аутентифікація та асоціація

Розглянемо процес підключення бездротового клієнта до бездротової мережі, працюючої в інфраструктурному режимі. Для того, щоб бездротовий пристрій став повноцінним членом бездротової мережі, тобто асоціювався з точкою доступу, він має послідовно пройти через чотири стани. [7]

Стан 1: початковий стан, не аутентифіковано, не асоційовано.

Стан 2: аутентифіковано, не асоційовано.

Стан 3: аутентифіковано і асоційовано (в очікуванні аутентифікації RSN).

Стан 4: аутентифіковано і асоційовано.

Діаграма станів показана на рисунку 1.2.

Для того, щоб бездротовий пристрій міг почати передачу даних через точку доступу, він має знаходитись в стані «аутентифіковано і асоційовано». Перехід в цей стан виконується поетапно шляхом обміну послідовностями кадрів керування 802.11.

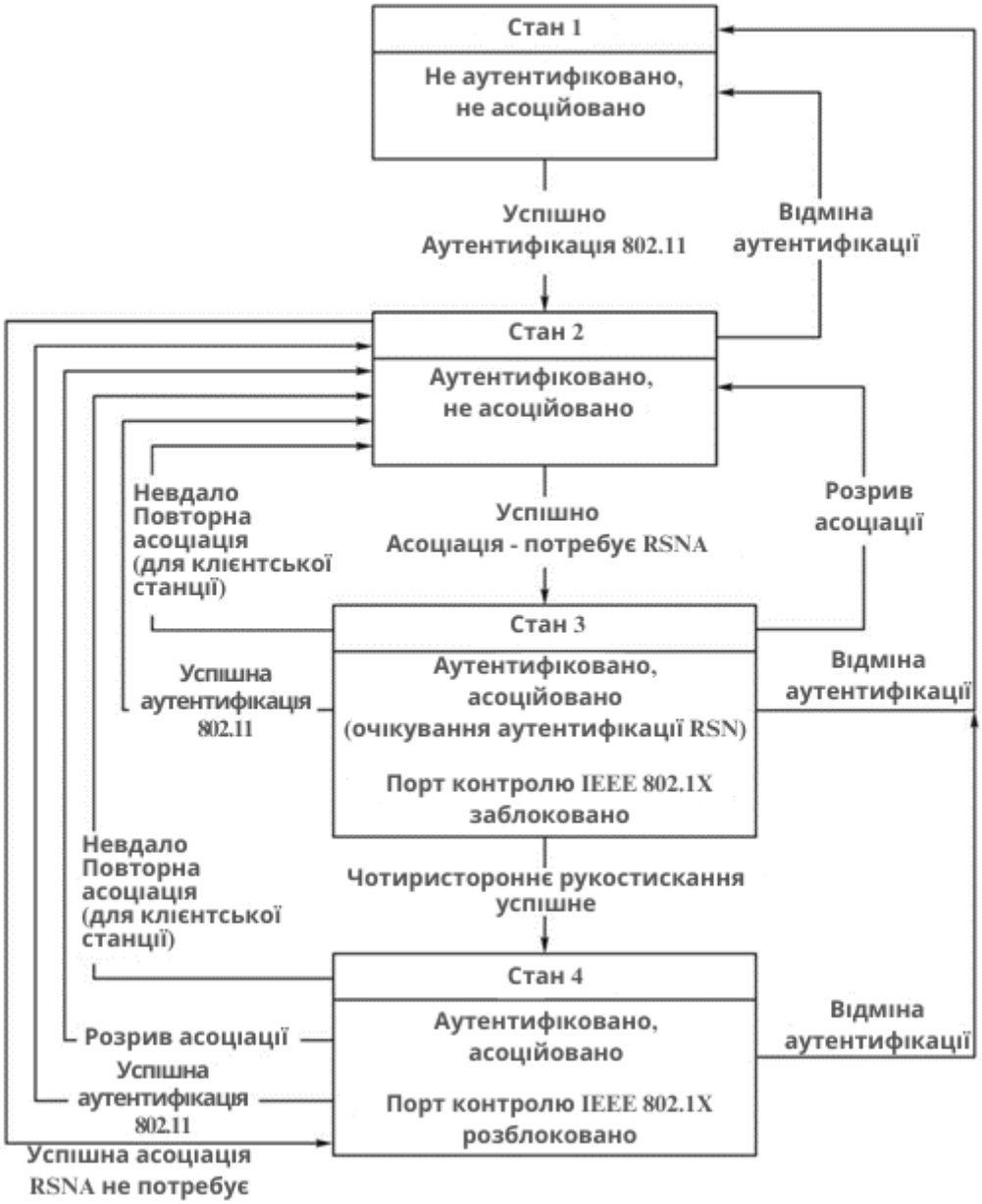

Рисунок 1.2 - Діаграма станів (машина станів) бездротового клієнта

Першою дією бездротового пристрою, який знаходиться в початковому стані, є виявлення бездротових мереж, в зоні дії яких він знаходиться. Клієнт відправляє фрейми пробного запиту (Probe Request). Точка доступу відповідає на пробний запит в тому випадку, якщо значення SSID (Service Set Identifier) співпадає з її особистим. Відповідь на пробний запит (Probe Response) містить інформацію про SSID, підтримці швидкостей передачі, типах шифрування і інших можливостей точки доступу. Він відправляється на індивідуальну адресу

станції, яка відправила запит. Після того, як станція обрала точку доступу для підключення, вона відправляє їй запит на аутентифікацію. [7]

В мережах IEEE 802.11 може використовуватись один з наступних типів аутентифікації:

- відкритих систем (Open System authentication);
- з загальним ключем (Shared Key authentication);
- при швидкому переході BSS (FT authentication);
- з використанням паролю (Simultaneous Authentication of Equals, SAE);
- на основі стандарту IEEE 802.1X-2004;
- на основі попередньо встановлених ключів (Pre-Shared key, PSK).

Стандарт 802.11 не нав’язує ніякої обов’язкової схеми аутентифікації, тому виробники обладнання можуть використовувати як небезпечні механізми аутентифікації, так і надійні. Вибір того чи іншого методу аутентифікації залежить від потреб до безпеки мережі, типу користувачів, котрі будуть отримувати доступ до мережі, типу даних, які будуть передаватися через неї. Але в будь-якому разі обов’язковою умовою для початку передачі фреймів між станцією і точко доступу є успішна асоціація та аутентифікація.

Аутентифікація відкритих систем і аутентифікація з загальним ключем відносяться до методів аутентифікації мереж, попередніх мережам з посиленим режимом безпеки (pre-RSN), тобто до методів, існуючих в оригінальному стандарті IEEE 802.11 (аутентифікація 802.11), маючого велику кількість вразливостей і не забезпечуючого аутентифікацію взаємодіючих приладів. У доповнення до методів безпеки, які існували в оригінальному стандарті, робоча група IEEE 802.11i розробила набір розширених функцій безпеки. В 2004 році стандарт IEEE 802.11i був ратифікований, і його фінальна форма отримала назву Robust Security Network (RSN) – мережу з посиленим режимом безпеки. Для надання послуг аутентифікації стандарт IEEE 802.11i опирається на IEEE 802.1X-2004 і механізм чотиристороннього рукостискання (4-Way Handshake), дозволяючи точкам доступу та бездротовим станціям безпечно обмінюватись ключами шифрування.

Для забезпечення конфіденційності і цілісності даних в стандарті визначені протоколи TKIP (Temporal Key Integrity Protocol) та CCMP (CTR with CBC-MAC Protocol). TKIP є необов'язковим і включений до стандарту для підтримки переходу з WEP на більш надійні протоколи. CCMP є обов'язковим для реалізації. Він заснований на алгоритмі шифрування AES (Advanced Encryption Standard) і більш стійкий до атак. В 2007 році стандарт IEEE 802.11i був включений в стандарт IEEE 802.11-2007.

А зараз розглянемо аутентифікацію на основі попередньо встановлених ключів, яка є найпоширенішим способом аутентифікації, що використовується в домашніх мережах та невеликих офісах. При аутентифікації на основі PSK на точці доступу і групі клієнтських станції, що підключаються до неї, потребується налаштування загального секрету, вид якого визначається ПЗ системи, що використовується. Секрет можна увести у виді строки з 64 шістнадцятирічних символів або у виді парольної фрази, що містить від 8 до 63 ASCII- символів. Для того, щоб створити ключ PSK довжиною 256 біти використовується спеціальна функція формування ключів, вхідними даними для якої є секрет, SSID мережі, в якій використовується цей секрет, довжина SSID, кількість ітерацій хешування і довжина ключа. Формування ключа PSK виконується до процесу обміну кадрами аутентифікації.

Почати процес аутентифікації може як точка доступу, так і станція, при цьому вони можуть зробити це одночасно. [6]

Після того, як станція отримує інформацію про політику безпеки точки доступу з фрейму Beacon чи за допомогою активного сканування, сторони обмінюються двома фреймами аутентифікації 802.11 з номерами послідовностей 0x0001 та 0x0002, та відправляють один одному повідомлення Commit, в якому міститься ймовірний секретний ключ другої сторони. У відповідь на це повідомлення, якщо секретний ключ збігся, кожна зі сторін посилає повідомлення Confirm з підтвердженням. На рисунку 1.3 показано процес аутентифікації на основі PSK.

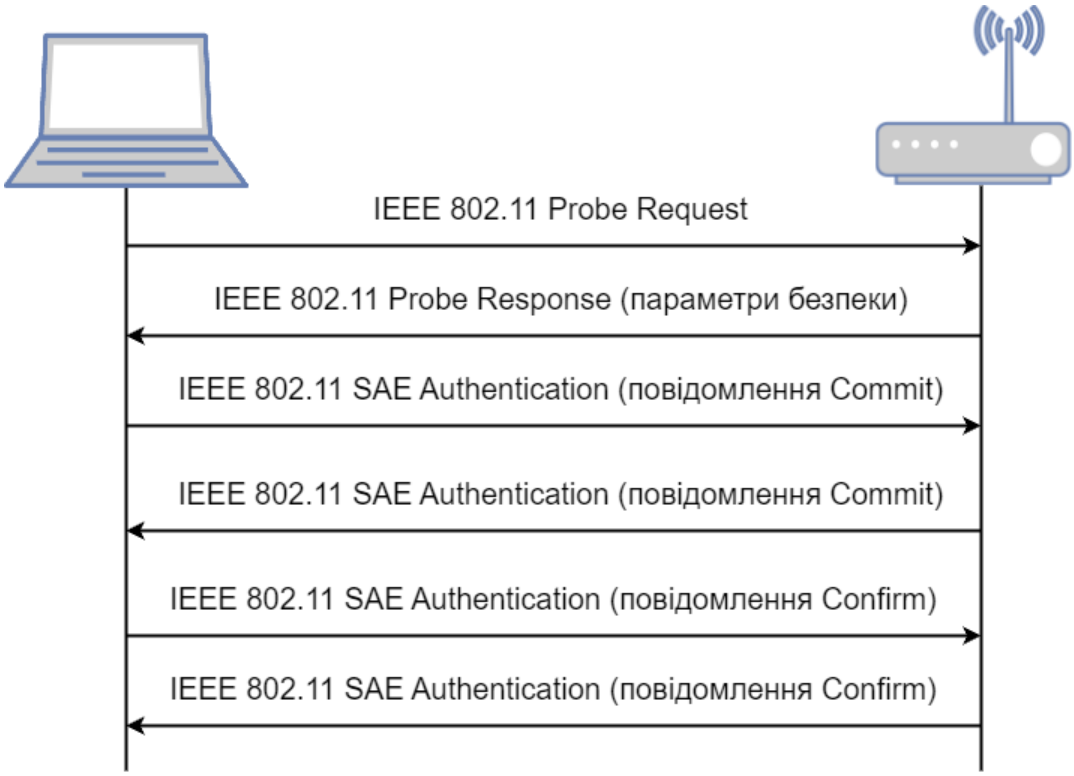

Рисунок 1.3 - Процес аутентифікації на основі PSK

Після успішної аутентифікації точка доступу і станція генерують із ключа PSK ключ PMK. Після чого станція асоціюється з точкою доступу і здійснюється домовленість про політику безпеки.

Згенерований в процесі аутентифікації ключ PMK використовується в процесі чотиристороннього рукостискання для генерації ключа PTK. Для шифрування і дешифрування широкомовного та групового трафіку точкою доступу генерується ключ GTK та додається на асоційованою з нею станцією. Після завершення цього процесу станція стає членом бездротової мережі і може почати безпечну передачу даних.

1.2.2 Безпека передачі даних в бездротових мережах

В дротових мережах передавати і отримувати дані можуть тільки фізично підключені до мережі станції. В бездротових мережах передавати і отримувати дані може будь-яка станція, яка знаходиться в зоні досяжності радіозв'язку інших пристроїв. Таким чином, дротові пристрої в якомусь сенсі забезпечують конфіденційність даних, обмежуючи число можливих отримувачів даних

приладами, які фізично підключені до мережі. Для того, щоб приблизити рівень безпеки бездротових мереж до рівня безпеки дротових мереж, в стандарті IEEE 802.11 визначені можливості захисту вмісту повідомлень, що передаються. Запобігання читання повідомлень тими, коми вони не призначаються, забезпечуючи послугою конфіденційності даних.

Для забезпечення конфіденційності та цілісності даних в стандарті IEEE 802.11 передбачені протоколи шифрування WEP, TKIP та CCMP. Протокол WEP відноситься до засобів безпеки бездротових мереж, що існують в оригінальному стандарті IEEE 802.11. В наш час не рекомендується використання протоколу WEP у зв'язку з його криптографічною вразливістю, але його підтримка присутня в сучасному обладнанні для зворотної сумісності з застарілими пристроями. Протоколи TKIP та CCMP відносяться до засобів безпеки RSN та визначені в стандарті IEEE 802.11i-2004.

Протокол CCMP (CTR with CBC-MAC Protocol) є обов'язковим для реалізації протоколом роботи сучасних бездротових пристроїв і заснований на режимі CCM (Counter Mode with CBC-MAC) алгоритму шифрування AES (Advanced Encryption Standard). [9]

Ініціатива у розробці AES належить Національному інституту стандартів і технологій (NIST) США, який запропонував спільноті криптологів розробити нові алгоритми шифрування з ціллю створення повністю відкритого і безкоштовного алгоритму симетричного шифрування, який доступний для широкого застосування. Вимоги до алгоритму: симетричний, блочний, має підтримувати довжину блока 128 біт та довжину ключа 128, 192 і 256 біт. В результаті тривалого процесу оцінки запропонованих алгоритмів в якості AES був обраний алгоритм Rijndael і визначений в FIPS PUB 197-2001.

При розгляді можливостей посилення механізмів шифрування даних в бездротових мережах інститут IEEE адаптував алгоритм AES спеціально для них.

Режим CCM (визначений в IETF RFC 3610) являє собою комбінацію режиму блоків шифру (CTR, counter) та коду аутентифікації повідомлення із блочного

шифру (Cipher Block Chaining Message Authentication Code, CBC-MAC). Ці режими використовуються для надання двох сервісів:

– цілісність повідомлень: для забезпечення цілісності і аутентифікації CCMP використовує CBC-MAC. При цьому захищається цілісність не тільки даних, але і обраної частини заголовку кадру;

– конфіденційність даних: для шифрування CCMP використовує режим CTR.

Для забезпечення конфіденційності і цілісності використовується один і той самий ключ AES довжиною 128 біт. CCM потребує «свіжий» тимчасовий ключ для кожної сесії і унікальні випадкові дані (nonce) для кожного кадру, що захищається даним тимчасовим ключем. Для створення nonce використовується номер пакету (PN) довжиною 48 біт, що дозволяє уникнути атак типу replay. Тимчасовий ключ генерується в процесі аутентифікації на основі стандарту IEEE 802.1X або PSK. [5]

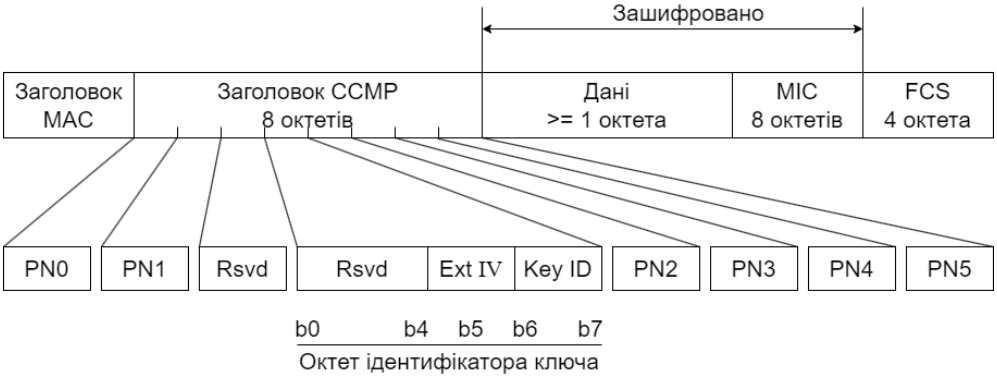

Рисунок 1.4 - Формат фрейму CCMP

Безпека бездротових мереж є вельми важливим питанням, тому в 2000 році Wi-Fi Alliance запустив програму сертифікації, яка визначає вимоги до безпеки бездротових мереж , включаючи підтримку WEP. Швидкий розвиток бездротових технологій, а також вразливість WEP привели до необхідності розробки нових механізмів захисту. В доповнення до функцій безпеки, що існували в оригінальному стандарті IEEE 802.11, робоча група IEEE 802.11i розробила набір розширених функцій безпеки. Для того, щоб прискорити їх використання в бездротових мережах, в 2003 році Wi-Fi Alliance представив

програму сертифікації **Wi-Fi Protected Access (WPA).** Вона ґрунтувалася на проекті стандарту IEEE 802.11i і представляла собою набір механізмів безпеки, які дозволяли вирішити більшість проблем з забезпеченням захисту мереж 802.11. Замість протоколу WEP в WPA використовувався протокол TKIP. Також WPA включала підтримку перевірки цілісності повідомлень. Аутентифікація виконувалась на основі протоколу IEEE 802.1X з EAP для корпоративних користувачів і на основі PSK для домашніх користувачів і користувачів невеликих офісів. [10]

В 2004 році стандарт IEEE 802.11i був ратифікований. Паралельно Wi-Fi Alliance представив програму сертифікації **WPA2**, засновану на WPA, але замість протоколу TKIP використовувала більш криптостійкий протокол шифрування CCMP. Аутентифікація також, як і в WPA, виконувалась на основі протоколів IEEE 802.1X з EAP чи PSK. З початку WPA2 була додатковою програмою сертифікації, але починаючи з 2006 року відповідність вимогам WPA2 є обов'язковим для всіх пристроїв Wi-Fi Certified. Варто зазначити, що WPA2 дозволяє захистити не тільки кадри даних, але і кадри керування. В таблиці 1.2 приведено порівняння функціональності WEP, WPA та WPA2. [8]

Таблиця 1.2 Порівняння функціональності WEP, WPA та WPA2

	WEP	WPA	WPA2
Протокол шифрування	Алгоритм RC4 з ручним призначенням ключів	Протокол TKIP, який базується на RC4	Протокол CCMP з ключами AES довжиною 128 біт
Цілісність даних	Лінійна хеш-функція	Криптографічна хеш-функція	
Управління ключами	Ні	Так	
Виявлення атак типу replay	Ні	Так	

У домашніх мережах та мережах невеликих офісів зазвичай використовують режим WPA/WPA2-Personal, оскільки в цьому випадку не потребується ніякого додаткового обладнання, окрім точки доступу і клієнтського пристрою. Ключ PSK в режимі WPA/WPA2-Personal отримують з SSID і парольної фрази, котра вказується в налаштуваннях пристрою. Для підвищення безпеки мереж рекомендується використовувати складні парольні фрази і якомога частіше оновлювати їх.

1.3 Засоби навчання студентів принципам захисту мереж Wi-Fi

Один із підходів до навчання – це використання сучасних методів, які дозволяють студентам отримати практичні навички в області безпеки Wi-Fi. Інтерактивні лекції, де акцент робиться на реальних випадках та сценаріях, можуть допомогти студентам зрозуміти принципи захисту мережі.

Лабораторні та практичні роботи відіграють ключову роль у формуванні навичок студентів. Наприклад, студенти можуть проводити експерименти з реальним обладнанням, налаштовувати параметри захисту, вивчати типові атаки та їх уникнення. Лабораторні роботи можуть включати в себе симуляцію атак для надання студентам можливості вивчати реальні сценарії безпеки Wi-Fi в контрольованому середовищі.

Використання спеціалізованого програмного забезпечення є необхідною складовою навчального процесу. Програми, такі як Wireshark та Aircrack-ng, дозволяють студентам вивчати та аналізувати трафік мережі, виявляти потенційні загрози та ефективно застосовувати принципи захисту.

Узагальнюючи, засоби навчання студентів принципам захисту бездротових мереж Wi-Fi повинні охоплювати різні аспекти, починаючи від теоретичного розуміння базових принципів до практичного використання програмних та апаратних інструментів. Це дозволяє студентам отримати комплексні знання та готовність до роботи в області безпеки мережі Wi-Fi.

1.4 Висновки

Безпека бездротових мереж Wi-Fi у сучасному світі має вирішальне значення. Їх зручність та широкий діапазон використання зробили їх популярними, але водночас виникла проблема вразливості до атак. Незалежно від стандарту захисту, відповідна конфігурація та своєчасне оновлення обладнання відіграють ключову роль.

Методи навчання, які комбінують теоретичне вивчення та практичний досвід через кейс-стадії, симуляції та роботу з реальним обладнанням, дозволяють студентам глибоко розуміти принципи безпеки Wi-Fi. Такий підхід не тільки гарантує засвоєння знань на практиці, але й показує студентам реальні наслідки їхніх рішень.

Увага до деталей, освіта та практичний досвід стають основними елементами підготовки фахівців з безпеки бездротових мереж. Тільки збалансований підхід до теорії та практики забезпечує здатність відповідати на виклики в сфері інформаційної безпеки.

2 ПРИНЦИПИ НАЛАГОДЖЕННЯ МОЖЛИВИХ МЕХАНІЗМІВ ЗАХИСТУ МЕРЕЖІ WI-FI НА ОБЛАДНАНІ КАФЕДРИ ЕОМ

2.1 Перелік та характеристики доступного обладнання

Існуюча мережева інфраструктура кафедри електронних обчислювальних машин була створена з огляду на потреби користувачів на момент розгортання. Вона містить різноманітні компоненти, зокрема сервери, робочі станції, комутатори та інше мережеве обладнання. Ці елементи взаємопов'язані між собою та забезпечують передавання даних і доступ до ресурсів.

Мережа кафедри інтегрована в університетську IT-інфраструктуру та підключена до головного серверу закладу. Це відкриває широкі можливості для спільного користування різноманітними ресурсами та сервісами університету. Також це сприяє ефективній взаємодії між кафедрою та іншими підрозділами університету.

Головний сервер університету забезпечує централізоване управління та зберігання різних ресурсів, таких як електронні бібліотеки, бази даних, навчальні матеріали, а також послуги, що надає університет, наприклад електронна пошта, відеоконференц-зв'язок, спільні сховища файлів тощо.

Кафедра електронних обчислювальних машин розташована на третьому поверсі університету і складається з сімнадцяти приміщень. Їх можна поділити на адміністративні та навчальні аудиторії. Адміністративні використовуються для організаційних функцій кафедри: кабінети викладачів, завыдуючого кафедрою чи секретаря. Навчальні призначені для лекцій, семінарів, практичних занять та лабораторних робіт зі студентами. Цей розподіл забезпечує ефективну роботу кафедри та комфортне навчання й діяльність студентів і викладачів.

Структура мережі кафедри ЕОМ відображена на рисунку 2.1, що надає візуальне уявлення про компоненти та їх взаємозв'язки в межах мережі.

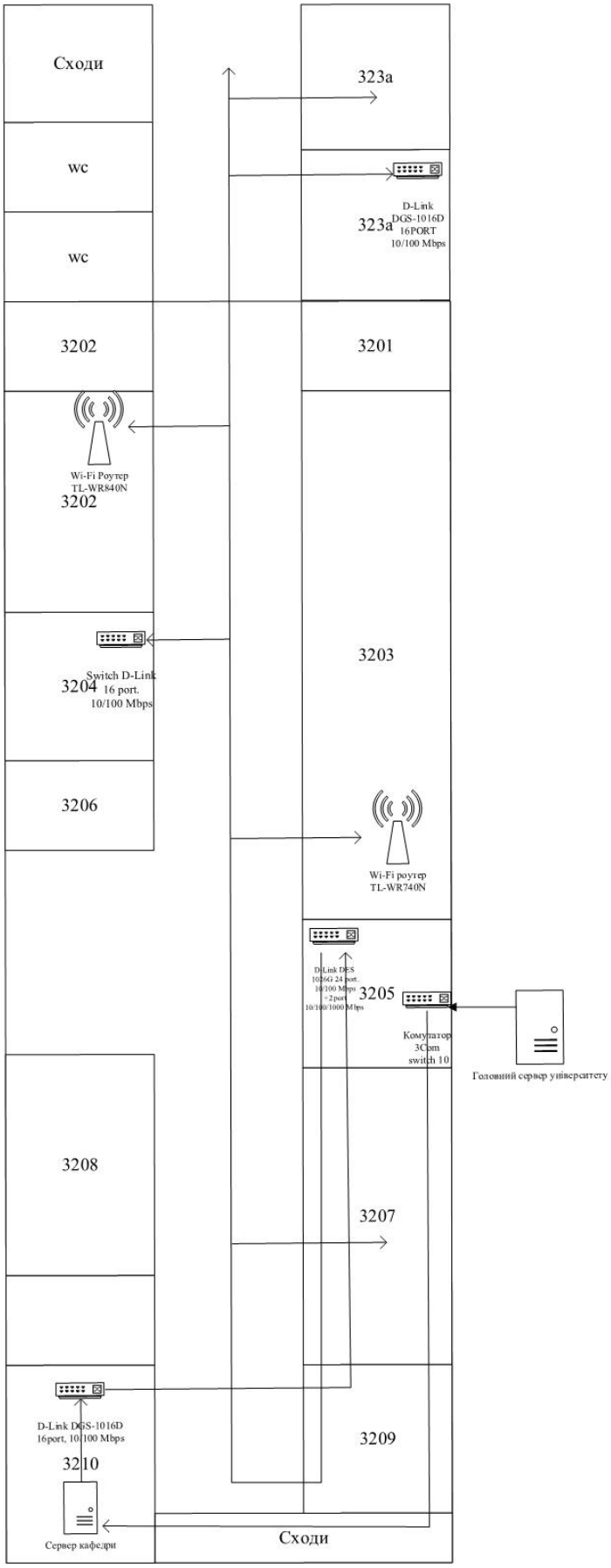

Рисунок 2.1 - Поточна структура мережі кафедри ЕОМ

Локальна мережа відділу розділена на кілька сегментів, що не поєднані між собою. Приміщення 3204, 3210 та 3205 утворюють внутрішню мережу, приєднану до сервера підрозділу. Ця внутрішня мережа створює окрему локальну інфраструктуру для зазначених аудиторій. Водночас інші кімнати на кафедрі під'єднані до зовнішньої мережі, котра є частиною інфраструктури університету. Це означає, що ці приміщення не можуть обмінюватися даними з комп'ютерами внутрішньої мережі.

У кімнатах 3202 та 3203 встановлено Wi-Fi роутери для бездротового під'єднання пристроїв до мережі цих аудиторій.

Кабельна система відділу повністю побудована за допомогою симетричного 4-парного мідного кабелю категорії 5, відомого як "неекранована кручена пара" або UTP. Для фізичного з'єднання комп'ютерів та пристроїв використовують конектори і розетки RJ-45, що гарантує надійне підключення та сумісність з більшістю мережевих пристроїв.

Загалом у локальній мережі відділу задіяні значні ресурси та устаткування. Наявні п'ятдесят комп'ютерів для роботи студентів і співробітників, а також один сервер для централізованого зберігання та обробки даних.

Для забезпечення зв'язку між пристроями використовують шість комутаторів D-Link DES та два комутатори 3Com OfficeConnect Dual Speed Switch 8.

Рисунок 2.2 – Комутатор D-link DES-1026G

Комутатор D-Link DES-1026G визначається як некерований пристрій, широко використовуваний в локальних мережах. За своєю функціональністю, він має 24 порти 10/100BASE-TX Fast Ethernet і 2 порти Gigabit Ethernet,

розширюючи можливості для підключення швидких та повільних пристроїв до мережі.

Однією з ключових переваг цього комутатора є його висока швидкість передачі даних, завдяки швидким портам Fast Ethernet та Gigabit Ethernet. Це дозволяє забезпечити ефективний обмін і надійне передавання інформації між пристроями в мережі. Додатково, наявність функції Quality of Service (QoS) гарантує пріоритет для певних видів трафіку, забезпечуючи високу якість обслуговування.

Незважаючи на ці переваги, комутатор D-Link DES-1026G має обмежені можливості в деяких складних мережевих сценаріях. Відсутність розширених функцій, таких як віртуальні локальні мережі (VLAN) та різноманітні функції мережевої безпеки, може ускладнити розгортання в ситуаціях, де необхідні додаткові можливості для налаштування та розширення мережі.

Також на кафедрі використовуються різні моделі маршрутизаторів та адаптерів, кожен з яких має свої особливості та переваги. Для об'єктивного оцінювання можливостей обладнання необхідно розглянути технічні характеристики кожного пристрою.

– Маршрутизатор TL-WR840N є однією з популярних моделей в серії від виробника TP-Link. За стандартом 802.11n він забезпечує швидкість передачі даних до 300 Мбіт/с. Оснащений двома зовнішніми антенами, що гарантує стабільний сигнал на великій території. Має також 4 порти LAN для дротового підключення пристроїв.

Рисунок 2.3 – Маршрутизатор TL-WR840N

– Маршрутизатор Netis WF2419 працює на стандарті 802.11n і забезпечує швидкість до 300 Мбіт/с. Відмінністю є підтримка двох діапазонів частот: 2,4 ГГц та 5 ГГц, що дозволяє ефективно оптимізувати передачу даних в завантажених мережах. За допомогою 5 портів Ethernet він забезпечує можливість дротового підключення. [15]

Рисунок 2.4 – Маршрутизатор Netis WF2419

– Маршрутизатор TP-Link TL-WR740N, порівняно з моделлю TL-WR840N, має більш обмежений функціонал, забезпечуючи швидкість до 150 Мбіт/с та обладнаний однією антеною. Завдяки своїм складним розмірам і простоті встановлення, він ідеально підходить для невеликих приміщень або тимчасових мереж. [16]

Рисунок 2.5 – Маршрутизатор TL-WR740N

– PCI-адаптер D-Link DWA-525 розроблений для настільних комп'ютерів і призначений для з'єднання їх з Wi-Fi мережами. Забезпечуючи швидкість до 150 Мбіт/с за стандартом 802.11n, цей адаптер від D-Link відрізняється підтримкою розширених заходів безпеки, включаючи WPA, WPA2 та WPS. [17]

Рисунок 2.6 – Адаптер D-Link DWA-525

У рамках нового міжнародного проекту на кафедру надійде точка доступу типу Wireless AC1300 Wave 2 Dual-band Unified Access Point, оснащена технологією PoE. З метою об'єктивної оцінки можливостей цього інноваційного обладнання розглянемо його технічні параметри та функціональні особливості.

Рисунок 2.7 – Wireless AC1300 Wave 2 Dual-band Unified Access Point with PoE

Точка доступу Wireless AC1300 Wave 2 Dual-band Unified Access Point with PoE володіє швидкістю передачі даних до 1300 Mbs, що є ідеальним параметром для обробки великих обсягів даних та потокового відео. Робота в обох діапазонах частот (2,4 ГГц та 5 ГГц) дозволяє оптимізувати передачу даних в залежності від навантаження мережі. Технологія Wave 2 дозволяє використовувати переваги високошвидкісного бездротового зв'язку, забезпечуючи ефективний обмін даними. [18]

Інтеграція технології PoE дозволяє живлення пристрою через Ethernet-кабель, спрощуючи процес встановлення та забезпечуючи більшу гнучкість в розташуванні. Пристрій також забезпечує технічну сумісність для інтеграції з різноманітним мережевим обладнанням та системами управління. Механізми шифрування та аутентифікації (WPA, WPA2, WPA3) гарантують високий рівень безпеки мережі.

Технологія Power over Ethernet (PoE) визначається своєю винятковою ефективністю та інноваційністю в галузі живлення мережевих пристроїв.

Вперше запропонована та стандартизована компанією Cisco, PoE став важливим кроком у розвитку мережевих технологій.

Однією з ключових переваг технології PoE є її гнучкість розташування пристроїв. Можливість передавати живлення через Ethernet-кабель дозволяє розміщувати пристрої в будь-якому місці, незалежно від доступу до електромережі. Це особливо актуально для точок доступу, камер відеоспостереження та інших мережевих пристроїв, розташованих в важкодоступних місцях.

Додатково, використання технології PoE спрощує інфраструктуру мережі, зменшуючи кількість кабелів і джерел живлення. Це призводить до оптимізації ресурсів та зменшення витрат електроенергії. Однією з інших переваг є простота обслуговування, оскільки єдина мережева інфраструктура об'єднує передачу даних та живлення.

Всі ці пристрої є важливими компонентами мережевої інфраструктури кафедри. Вони забезпечують високу швидкість та надійність з'єднання, дозволяючи студентам і викладачам ефективно взаємодіяти з мережевими ресурсами.

2.2 Покрокове налаштування протоколів безпеки на точках доступу

Першочергове, що необхідно зробити, це зміна стандартного імені та паролю для доступу до налаштувань роутеру. Пароль захистить від несанкціонованого доступу до роутеру сторонніх людей. Після зміни паролю ніхто не зможе підключитись до інтерфейсу та змінити налаштування нашої мережі.

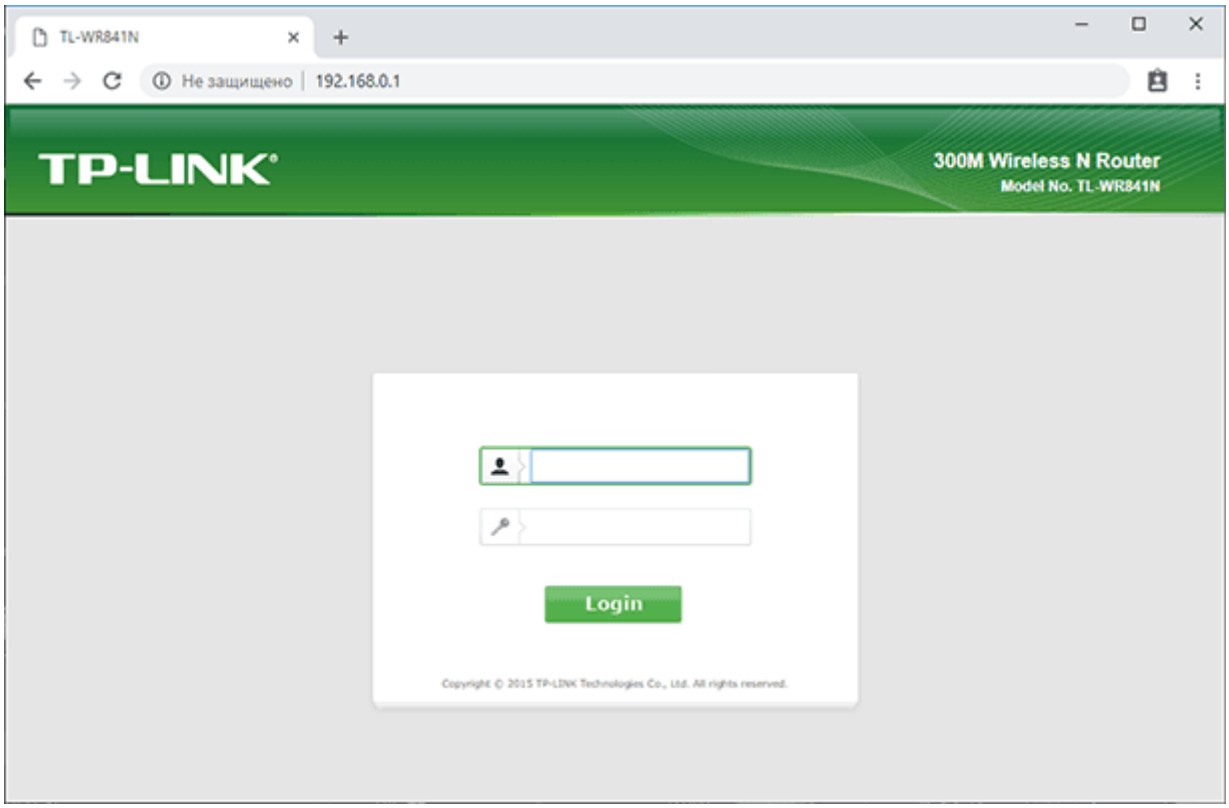

Рисунок 2.8 – Вікно входу до веб-інтерфейсу налаштувань роутера

Для цього необхідно ввести мережевий адрес маршрутизатора, який зазвичай вказаний на наклейці на його нижній частині. Після чого вводимо ім’я та пароль, який також вказаний на наклейці.

Потрапляємо в веб-інтерфейс налаштувань роутера, де ми можемо змінити стандарті ім’я та пароль входу у веб-інтерфейс, пароль для підключення до Wi-Fi мережі, налаштувати саму мережу, її режим роботи та захист, а також багато чого іншого.

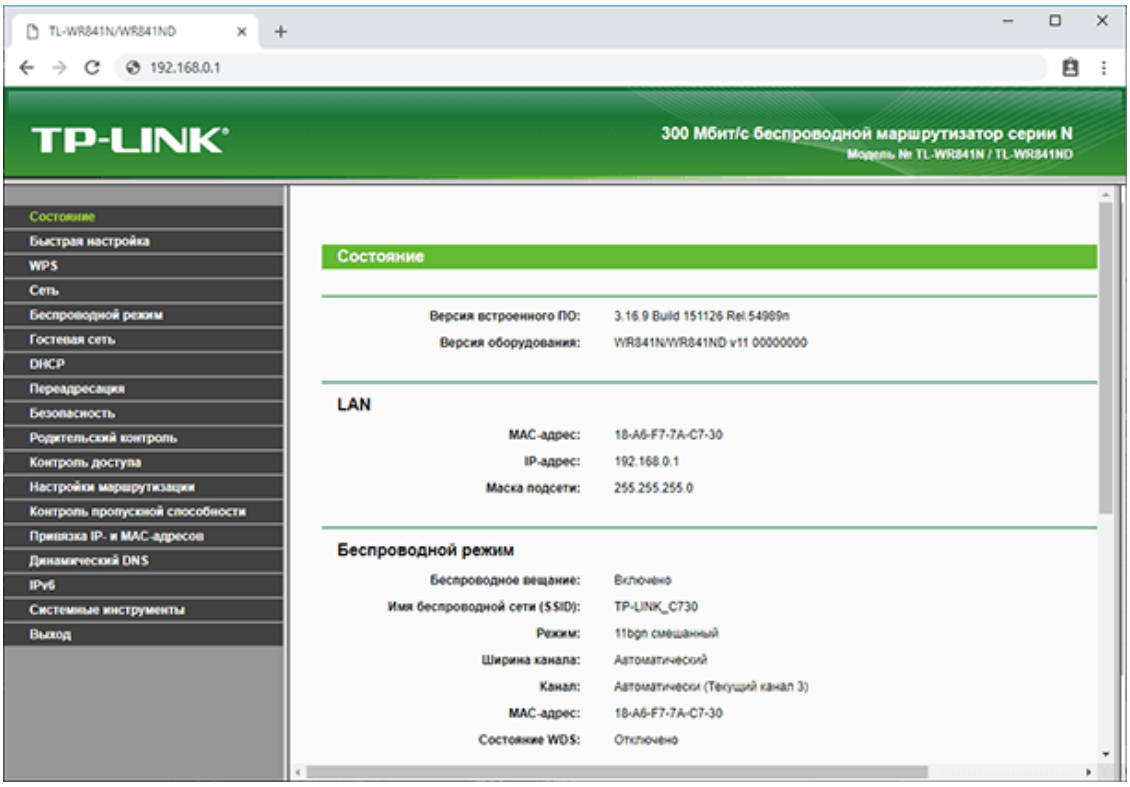

Рисунок 2.9 – Вікно веб-інтерфейсу налаштувань роутера

Переходимо у вкладку «Системні інструменти» («System tools») і знаходимо пункт «Пароль» (чи «Password»).

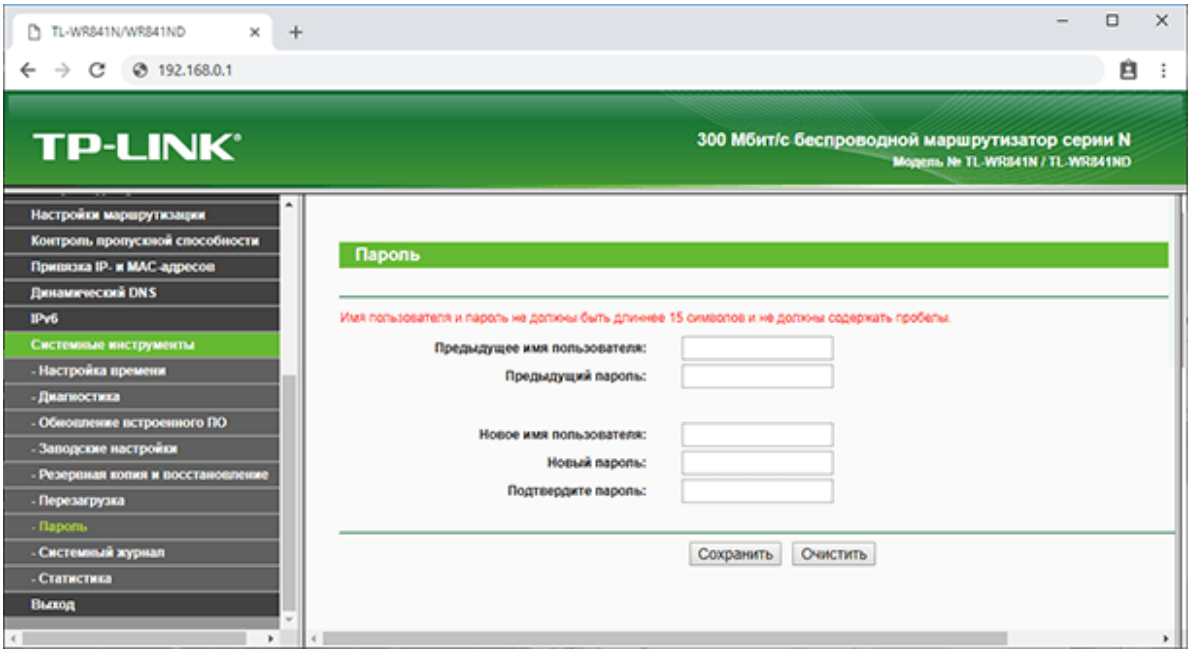

Рисунок 2.10 – Вкладка «Системні інтсрументи» веб-інтерфейсу налаштувань роутера

Тут нам необхідно буде вказати наші попередні ім’я та пароль, після чого ввести нові та натиснути кнопку «Зберегти» («Save»). От і все, пароль доступу до веб-інтерфейсу налаштувань роутеру змінено. Перший пункт по налаштуванню безпеки виконано. Йдемо далі.

Другий важливий момент – це встановлення паролю до нашої Wi-Fi мережі а також налаштування протоколу безпеки та типу шифрування. Це забезпечить надійність мережі а також безпечність її використання.

Для цього переходимо у вкладку «Бездротовий режим» («Wireless»). І знаходимо пункт «Захист бездротового режиму» («Wireless Secutirty»).

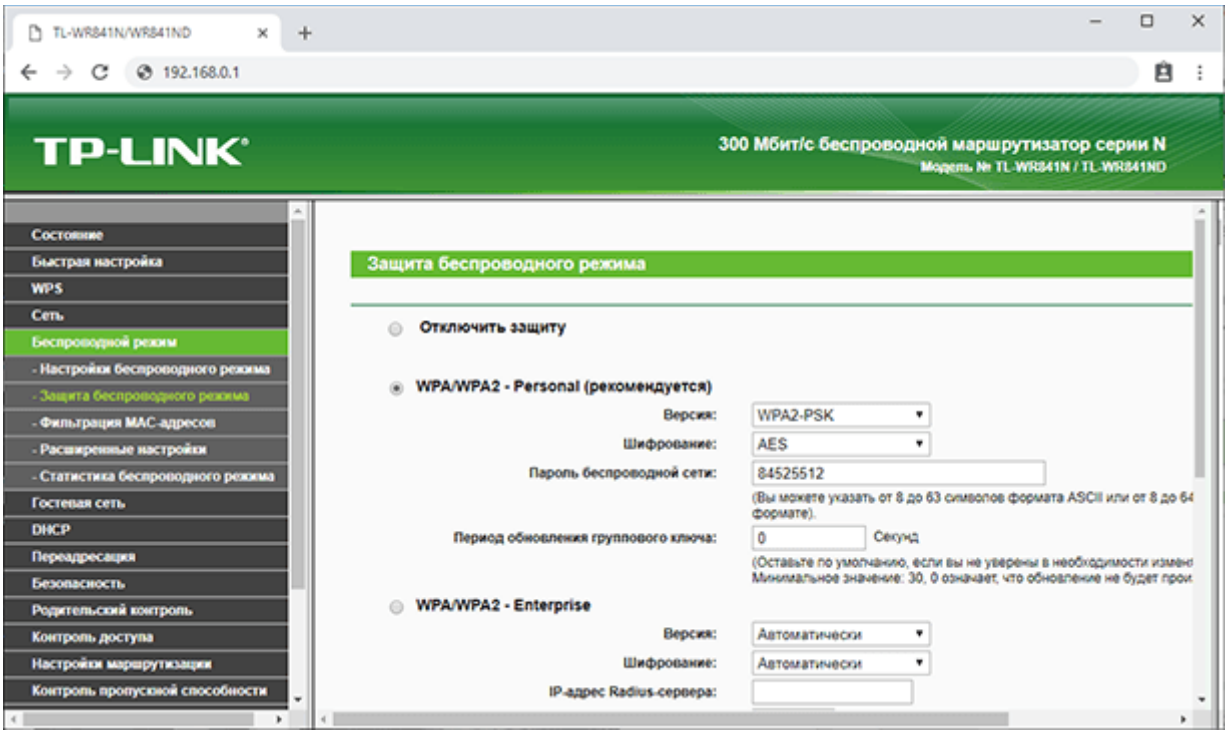

Рисунок 2.11 – Вкладка «Бездротовий режим» веб-інтерфейсу налаштувань роутера

Якщо захист бездротової мережі вимкнено – вмикаємо його. Для цього обираємо одну з запропонованих опцій захисту. Для нас буде достатньо рекомендованого захисту «WPA/WPA2-Personal». Тип шифрування обираємо «AES», так як з минулого розділу ми знаємо, що він є більш надійним та захищеним.

Вводимо бажаний пароль в поле «Пароль бездротової мережі» («Wireless Password»). Пароль має бути «міцним», бажано щоб він містив як цифри, так і букви з символами. Це забезпечить надійний захист та не дасть можливості злому з перебором паролів.

Наступним важливим налаштування є відключення функції WPS. Ця функція дозволяє швидко підключатись до бездротової мережі без необхідності вводу паролю. На практиці функцією WPS мало хто користується і вона є вкрай нестійкою до злому, тому рекомендується її вимкнути.

Для цього переходимо у вкладку «WPS» і обираємо «Відключити» («Disable WPS»).

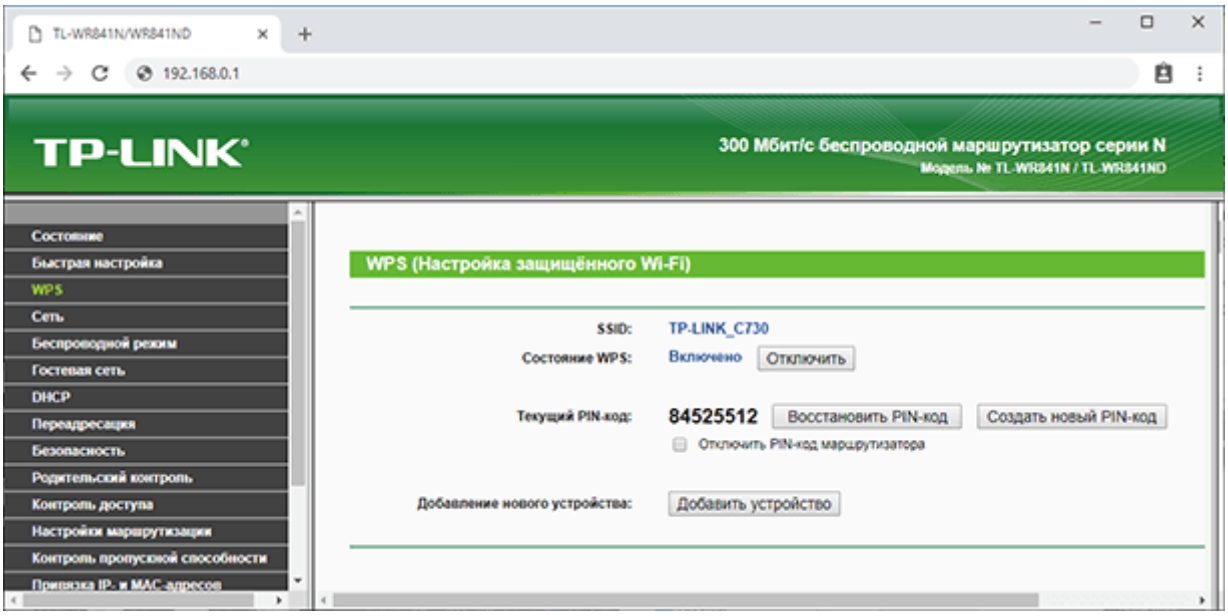

Рисунок 2.12 – Вкладка «WPS» веб-інтерфейсу налаштувань роутера

Варто також зазначити про ще одне налаштування безпеки, яке може бути використане – шифрування SSID, тобто неможливість бачити ім’я бездротової мережі пристроях, що ведуть пошук Wi-Fi мереж. Але в умовах університетської кафедри використання цього налаштування не є раціональним та доцільним.

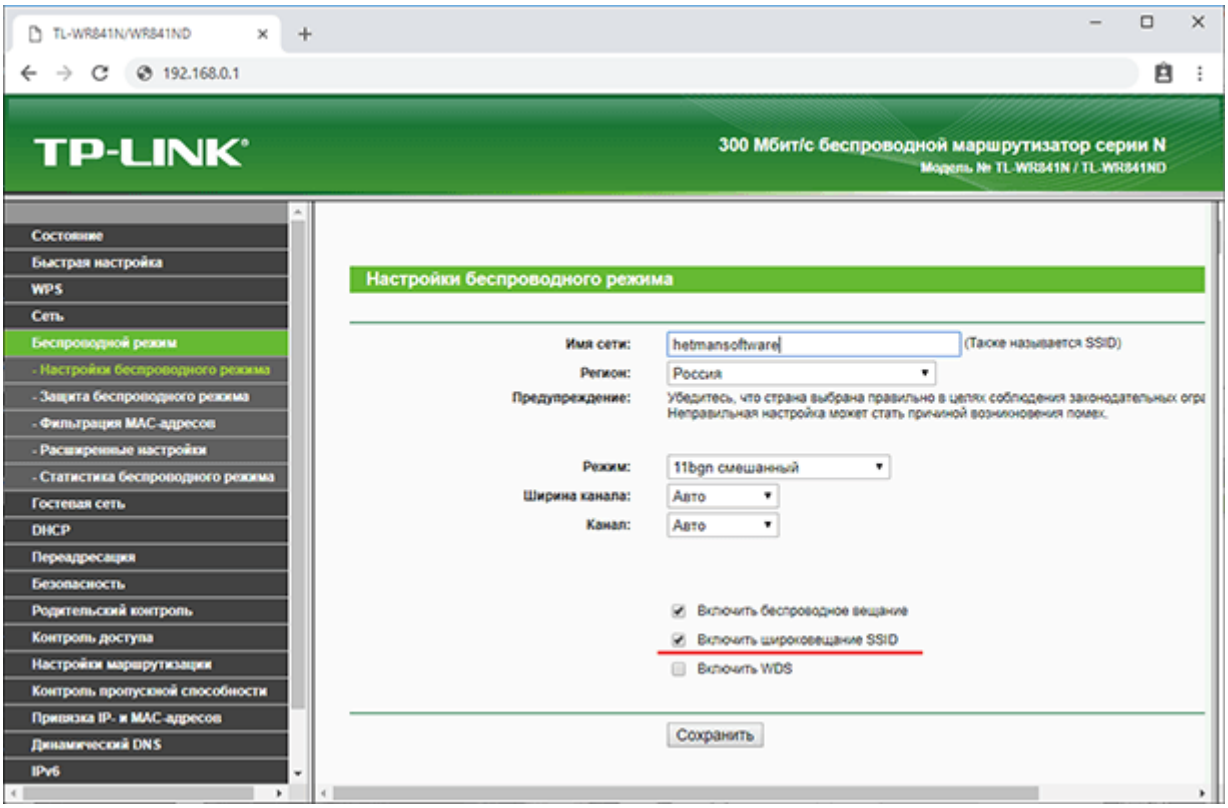

Рисунок 2.13 – Можливість шифрування SSID мережі в налаштуваннях роутеру

Ще один дієвий спосіб захисту який можна увімкнути в налаштуваннях роутеру є фільтрація пристроїв по MAC та IP адресі, але який також не є доцільним для використання в умовах університетської кафедри. Використання фільтрації по MAC-адресі та IP-адресі може бути не ефективним в умовах великої кількості пристроїв та користувачів на кафедрі. Підтримка та оновлення списків дозволених адрес може стати проблемою при збільшенні кількості пристроїв у мережі. Додавання нових пристроїв до списку фільтрації може вимагати значних зусиль адміністратора мережі. Окрім того, такий підхід ускладнює життя користувачів, оскільки вони повинні чекати на додавання свого пристрою до списку.

На кафедрі університету склад пристроїв може змінюватися досить часто через викладання, дослідження та проектну діяльність. Використання фільтрації може стати неефективним у таких умовах, де потрібно постійно вносити зміни.

2.3 Висновки

Під час аналізу обладнання та його налаштування було виявлено, що використання фільтрації по MAC-адресі та фільтрації по IP для бездротової мережі, що розташована на кафедрі університету, є менш доцільним підходом.

Фільтрація по MAC-адресу може призвести до адміністративних труднощів, оскільки вимагатиме постійного оновлення списків доступу при кожній зміні обладнання чи підключенні нових пристроїв. Це може створити непотрібну рутину та ускладнити управління мережею.

Щодо використання протоколу WPA-2, його ефективність вже засвідчена і призначена для створення надійного шару захисту в бездротових мережах. Застосування WPA-2 з правильними параметрами шифрування та складними паролями надає високий рівень конфіденційності та інтегрітету даних.

Таким чином, підбір оптимальних засобів захисту є ключовим етапом у створенні безпечної мережі, і в даному випадку, відмова від використання фільтрації по MAC-адресу та інших надто рутинних методів виявляється більш доцільною стратегією.

3 ДОСЛІДЖЕННЯ РОБОТИ МЕХАНІЗМІВ ЗАХИСТУ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI

3.1 Підбір інструментів для моніторингу мережі після налаштування

3.1.1. Операційна система – дистрибутив Ubuntu Linux

Ubuntu Linux, в якості операційної системи, демонструє високу ефективність та зручність для досліджень роботи та безпеки бездротових мереж Wi-Fi. Своєрідність цієї операційної системи полягає в декількох аспектах, що роблять її особливо підходящою для цих цілей. [19]

а) *Відкритий вихідний код***:** Ubuntu Linux є продуктом з відкритим вихідним кодом, що означає доступність ісходного коду для користувачів. Це важливо для дослідження та вивчення принципів, які використовуються у системі безпеки Wi-Fi. Студенти можуть отримати глибше розуміння роботи різних частин операційної системи.

б) *Зручний інтерфейс***:** Ubuntu має інтуїтивно зрозумілий та зручний для використання інтерфейс. Це полегшує налаштування та конфігурацію параметрів мережі. Зокрема, для досліджень у галузі безпеки Wi-Fi, коли необхідно взаємодіяти з різними налаштуваннями мережевих пристроїв, простота інтерфейсу є важливим фактором.

в) *Підтримка інструментів безпеки***:** Ubuntu легко інтегрується з інструментами безпеки, такими як Aircrack-ng і Wireshark, що надає можливість вивчення та тестування захисту мережі. Це стає важливим фактором для практичного опанування методів обійдення та аналізу безпеки вайфай.

г) *Стабільність та надійність***:** Ubuntu відома своєю стабільністю та надійністю роботи. Це важливо для проведення експериментів та досліджень, оскільки система повинна надійно функціонувати, щоб результати були достовірними.

Отже, Ubuntu Linux, завдяки своїм технічним особливостям та підтримці інструментів безпеки, стає ефективним інструментом для проведення лабораторних робіт та досліджень в галузі безпеки Wi-Fi мереж.

Рисунок 3.1 - Робочий стіл дистрибутиву Ubuntu Linux

3.1.2. Aircrack-ng

Aircrack-ng є важливим інструментом для досліджень та тестування безпеки бездротових мереж Wi-Fi в університетських лабораторіях. Завдяки своїм функціональним можливостям, він стає корисним інструментом для студентів і дослідників, які вивчають принципи захисту Wi-Fi мереж. [13]

Основні переваги використання Aircrack-ng включають:

– *Атаки на різні протоколи*: Інструмент підтримує атаки на різні протоколи шифрування, такі як WEP, WPA, та WPA2/WPA3. Це дозволяє студентам отримати практичний досвід роботи з різними видами захисту.

– *Сканування мереж*: Aircrack-ng дозволяє проводити активне та пасивне сканування Wi-Fi мереж, що є важливим для визначення доступних мереж та їх конфігурації.

– *Інтеграція з іншими інструментами*: Можливість взаємодії з іншими інструментами полегшує проведення комплексних досліджень та дозволяє автоматизувати деякі процеси.

– *Підтримка різних операційних систем:* Aircrack-ng є багатоплатформеним інструментом, що дозволяє використовувати його на різних операційних системах, забезпечуючи гнучкість використання.

– *Відкритий вихідний код:* Будучи проектом з відкритим вихідним кодом, Aircrack-ng стає об'єктом для вивчення та аналізу, що сприяє розвитку та внесенню внеску в галузь безпеки мереж.

Загалом, Aircrack-ng є ефективним інструментом для проведення лабораторних робіт та досліджень з безпеки Wi-Fi мереж, дозволяючи отримати глибоке розуміння принципів захисту та вразливостей мережевих технологій.

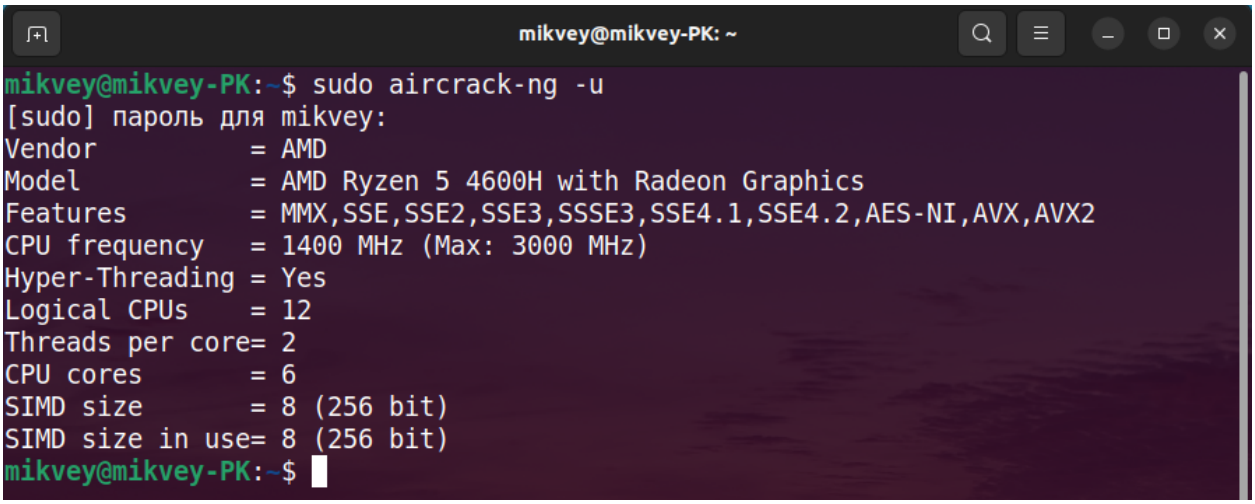

Рисунок 3.2 - Aircrack-ng в терміналі Ubuntu Linux

3.1.3. Wireshark

Це важливий інструмент для дослідження механізмів безпеки бездротових мереж Wi-Fi та вивчення їх роботи в університетських лабораторіях. Цей аналізатор мережевого трафіку надає студентам та дослідникам можливість докладно вивчати пакети даних, що передаються в бездротових мережах, та проводити аналіз їх структури та взаємодії. [12]

Основні характеристики та переваги використання Wireshark у контексті безпеки Wi-Fi:

Wireshark надає можливість перехоплювати та аналізувати пакети даних, які передаються в бездротових мережах. Це особливо важливо для вивчення

механізмів шифрування та безпеки, оскільки дозволяє ретельно розглядати структуру зашифрованих та незашифрованих пакетів.

Інтерфейс Wireshark інтуїтивно зрозумілий, що полегшує його використання студентами та дослідниками без значного попереднього досвіду в області мережевих технологій.

Можливість фільтрації трафіку за різними критеріями (протоколами, IP-адресами, портами) дозволяє концентруватися на конкретних аспектах мережевої діяльності, що полегшує аналіз інцидентів та пошук можливих загроз.

Wireshark дозволяє вивчати та аналізувати протоколи безпеки, такі як WEP, WPA, WPA2/WPA3, що надає можливість студентам ознайомитися з різноманітними заходами безпеки в Wi-Fi мережах.

Здатність зберігати історію перехопленого трафіку та відтворення його аналізу для подальшого вивчення робить Wireshark потужним інструментом для дослідження та навчання.

Загалом, Wireshark стає важливим засобом для поглибленого вивчення принципів безпеки та функціонування бездротових мереж Wi-Fi в університетському середовищі.

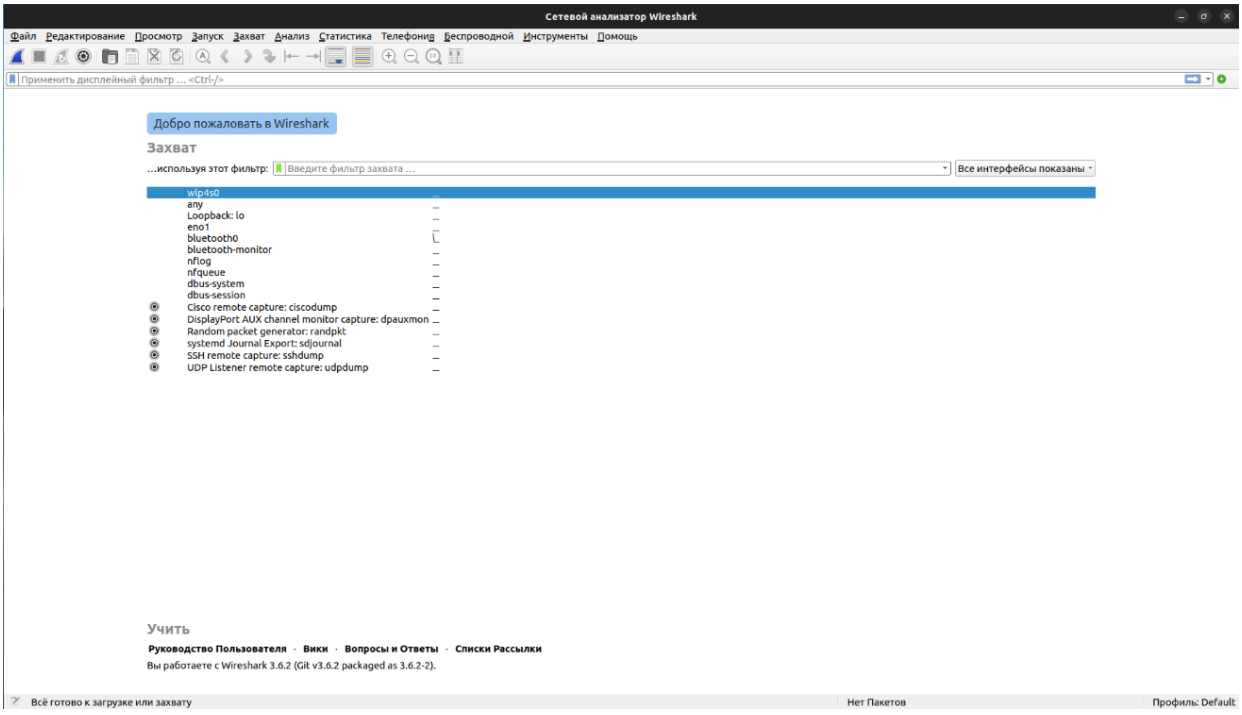

Рисунок 3.3 - Інтерфейс програми Wireshark

3.2 Використання інструментів для моніторингу та збирання даних стану мережі

Ніяких попередній дій та налаштувань не потрібно проводити в самій операційній системі Ubuntu Linux, лише встановити Aircrack-ng та Wireshark, що достатньо легко можна зробити через термінал Linux.

Тепер ми можемо відкрити термінал та подивитись список бездротових мережевих інтерфейсів встановлених в системі за допомогою команди *iwconfig*. Список бездротових мережевих інтерфейсів встановлених в нашій системі показані на рисунку 3.4.

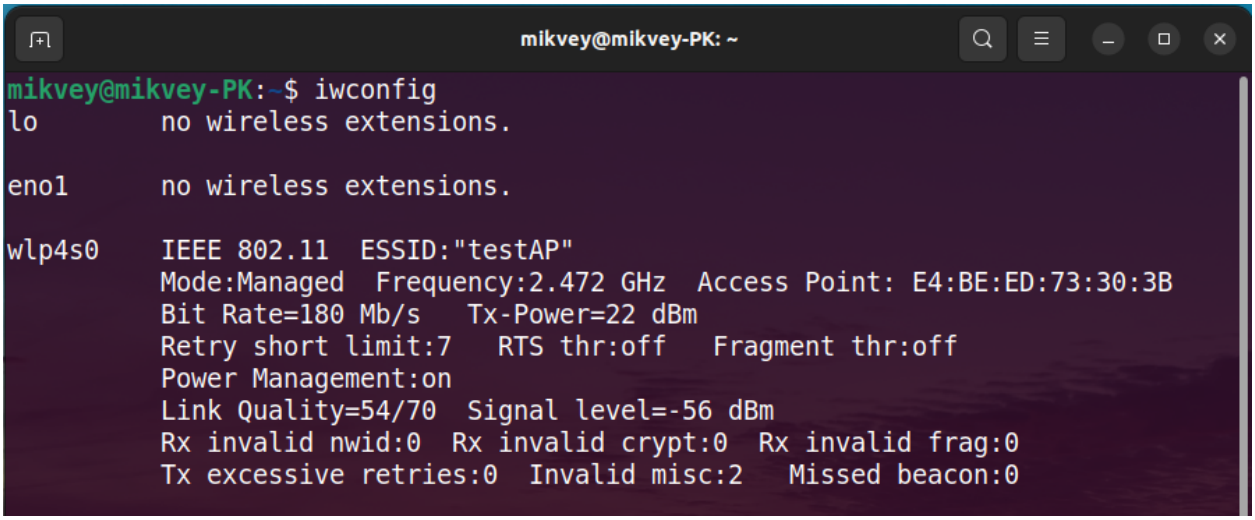

Рисунок 3.4 - Список бездротових мережевих інтерфейсів

На цьому рисунку ми бачимо назву нашого мережевого інтерфейсу – *wlp4s0*, а також режим його роботи – *Managed*. Це означає, що інтерфейс працює в керованому режимі, що дозволяє йому знаходити точки доступу, підключатись/відключатись до них та мати доступ до мережі Інтернет.

Нам необхідно перевести інтерфейс в режим роботи *Monitor*, після чого ми отримаємо можливість прослуховувати весь Wi-Fi трафік в області дії мережевого адаптера. Зробити це можна за допомогою команди в терміналі *airmon-ng start wlp4s0* (рисунок 3.5).

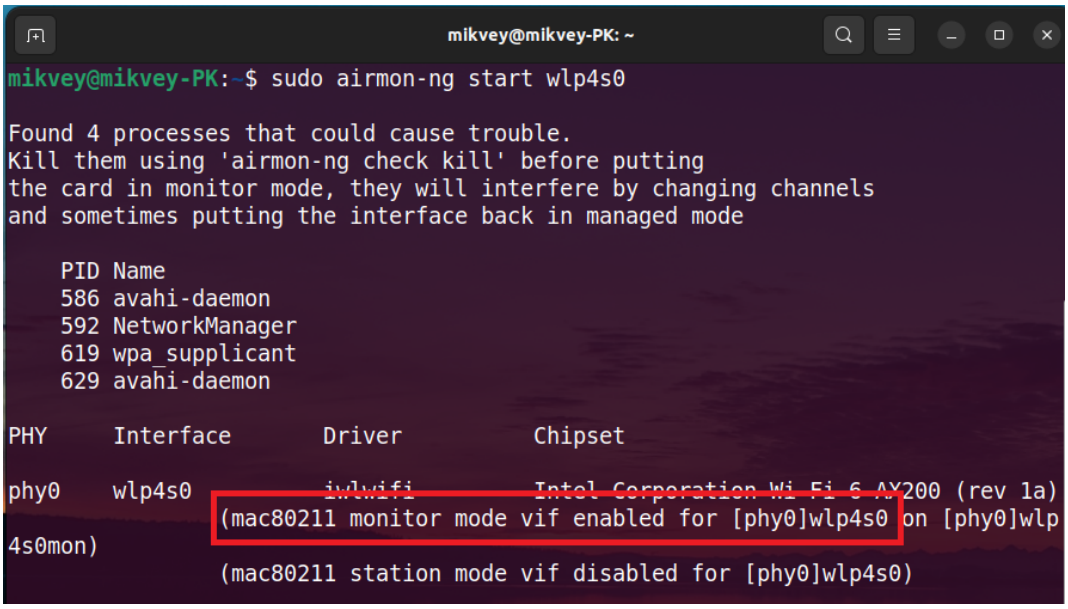

Рисунок 3.5 – Переведення бездротового мережевого адаптера в режим «Monitor»

Як ми бачимо з передостаннього рядка, у виділеній червоним області, наш інтерфейс переведено в режим моніторингу. А його ім’я змінилось на *wlp4s0mon* з приставкою «mon», що означає моніторинг. Наступним кроком ми дізнаємось які точки доступу є в зоні доступу мережевого адаптера та детальну інформацію про них. Для цього вводимо в терміналі таку команду – *airodump-ng wlp4s0mon* і спостерігаємо наступне (рисунок 3.6):

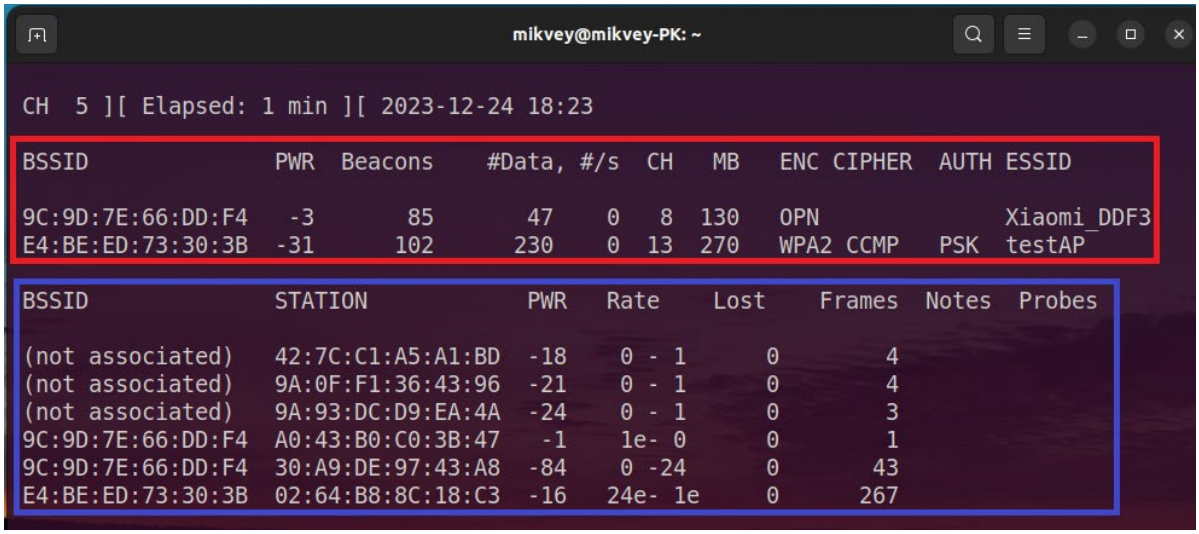

Рисунок 3.6 – Моніторинг бездротових точок доступу

Тут ми можемо побачити яскраво виражені дві таблиці. Перша з інформацією про наявні точки доступу, які діють в радіусі моніторингу нашого бездротового адаптера, а в другій – клієнтів, котрі під'єднані до точок доступу та обмінюються з ними пакетами. Для систематизації інформації та розуміння які дані містяться в конкретному стовпчику було побудовано дві таблиці. Відповідно: «Таблиця 3.1» - містить інформацію, що виділена червоним кольором на рисунку 3.6, «Таблиця 3.2» - інформацію, що виділена синім кольором.

Таблиця 3.1 – Інформація про знайдені точки доступу

BSSID	MAC-адреса точки доступу
PWR	Якість сигналу, коли обрано канал, інколи сила сигналу
Beacons	Показує кількість Beacons
Data	Кількість отриманих фреймів даних
CH	Канал на якому працює точка доступу
MB	Швидкість чи режим точки доступу
ENC	Протокол безпеки: opn – шифрування відсутнє, wep: wep шифрування, wpa: wpa або wpa2, wep?: wep або wpa
CIPHER	Тип шифрування
AUTH	Спосіб аутентифікації
ESSID	Ім'я мережі (в деяких випадках може бути скрито)

Таблиця 3.2 – Інформація про знайдених клієнтів підключених до мережі

BSSID	MAC-адреса з якою клієнт асоціюється у даної точки доступу
STATION	MAC-адреса самого клієнта
PWR	Сила сигналу
Frames	Кількість отриманих фреймів даних
Probes	Імена мереж (ESSID), котрі цей клієнт вже апробував

З отриманих даних ми можемо дізнатись, що наша тестова точка доступу має ім’я – testAP, MAC-адресу – E4:BE:ED:73:30:3B, працює на каналі 13, захищена протоколом безпеки WPA2 з типом шифрування CCMP та способом аутентифікації Pre-Shared Key.

А зараз ми проведемо кілька дослідів, щоб дізнатись як шифрування W-Fi мережі впливає на можливість моніторингу зловмисником фреймів, що передаються між нашими точкою доступу «testAP» та мобільним телефоном. А також переглянемо процес їх аутентифікації в обох випадках – з шифруванням та без шифрування мережі. Тож в цьому розділі будуть проведені наступні дослідження:

Дослід 1. Перехоплення кадрів Wi-Fi в незахищеній бездротовій мережі.

Дослід 2. Перехоплення кадрів Wi-Fi в захищеній бездротовій мережі.

3.2.1 Дослід №1

Для цього спочатку відключимо в налаштуваннях роутеру шифрування, позбавивши точку доступу безпечності і переглянемо трафік у Wi-Fi мережі через програму Wireshark.

Тож запускаємо Wireshark і потрапляємо на головну сторінку. Тут ми бачимо різні дротові/бездротові мережеві інтерфейси, але нам потрібен «wlp4s0mon», який раніше ми налаштували в режим моніторингу. (рисунок 3.7)

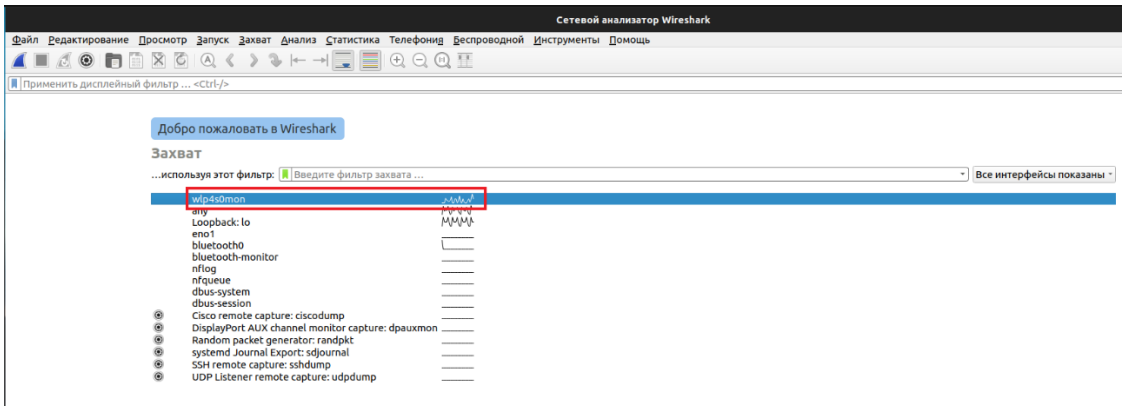

Рисунок 3.7 – Головна сторінка Wireshark

Подвійним натисканням на нього запускаємо прослуховування Wi-Fi мережі та спостерігаємо які кадри в ній передаються. З мобільного телефону ми

підключаємось до мережі та деякий час здійснюємо різноманітні операції в браузері. Після цього зупиняємо захоплення кадрів та зберігаємо файл моніторингу для його подальшого аналізу, котрий буде проведено в наступному пункті цього розділу.

Натискаємо «Файл»(1), далі натискаємо «Зберегти»(2), після чого вводимо бажане ім’я файлу та натискаємо кнопку «Зберегти»(3) (рисунок 3.8).

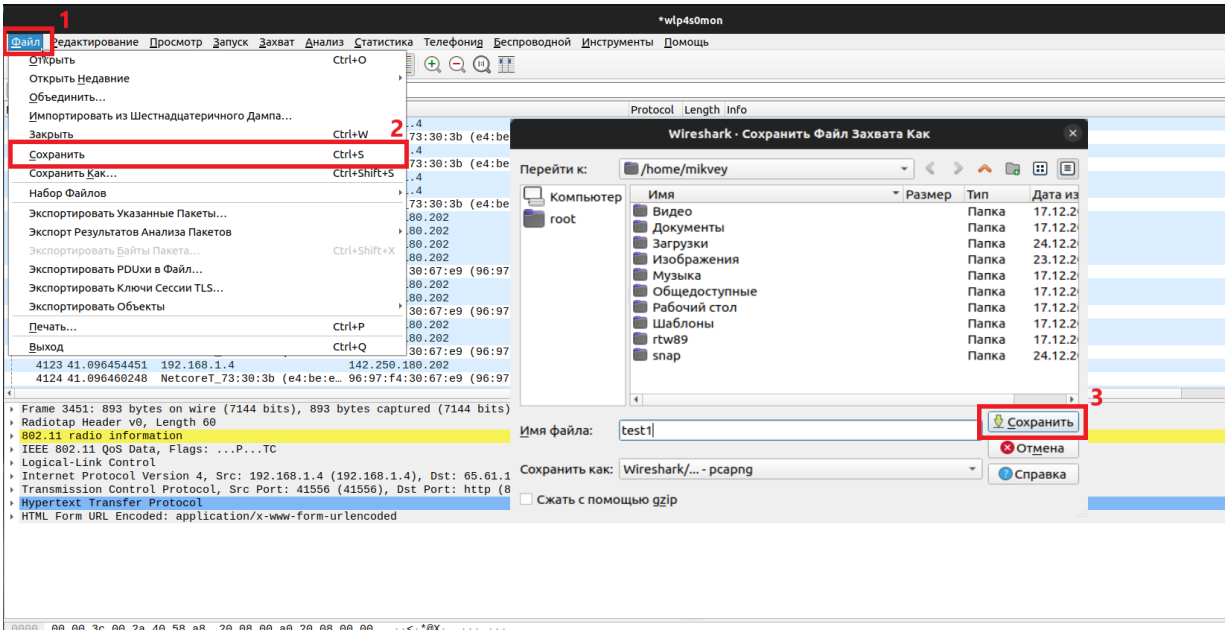

Рисунок 3.8 – Зберігання файлу перехоплених кадрів у Wireshark

3.2.2 Дослід №2

Що ж, тепер ми можемо налаштувати безпекові параметри на точці доступу для того, щоб дізнатись чи шифруються кадри та проаналізувати, що бачитиме зловмисник якщо ми надійно захистимо нашу Wi-Fi мережу. Вмикаємо протокол безпеки WPA/WPA2 та вводимо надійний пароль, ці дії більш детальніше описані в другому пункті другого розділу.

Після цього відтворюємо ті самі дії у Wireshark та прослуховуємо мережу уже із налаштованою безпекою. На мобільному телефоні знову підключаємось до точки доступу та здійснюємо якісь дії у браузері. Зупиняємо захоплення кадрів та зберігаємо файл.

Для аналізу процесу аутентифікації між користувачем та точкою доступу нема потреби в окремому перехопленні кадрів, адже інформації в тих файлах, що

ми отримали з наших двох дослідів, достатньо для того, щоб побачити як проходить аутентифікація та які кадри відправляються/отримуються при цьому.

Тепер ми маємо достатньо інформації з наших досліджень щоб провести аналіз зібраних даних. Переглянемо, що може побачити зловмисник, які персональні дані може перехопити та яку інформацію про нас дізнатись.

3.3 Аналіз зібраних даних

Для аналізу нами було сформовано 2 файли з перехопленими кадрами, котрі ми могли бачити в режимі реального часу під час моніторингу мережі. Але для зручності ми їх зберегли, щоб провести конструктивне порівняння.

3.3.1 Аналіз зібраних даних досліду №1

Тож відкриваємо перший файл з кадрами, які не були захищенні шифруванням. Для цього натискаємо «Файл» (1), після чого «Відкрити» (2), далі обираємо потрібний файл та натискаємо кнопку «Відкрити» (3) (рисунок 3.9).

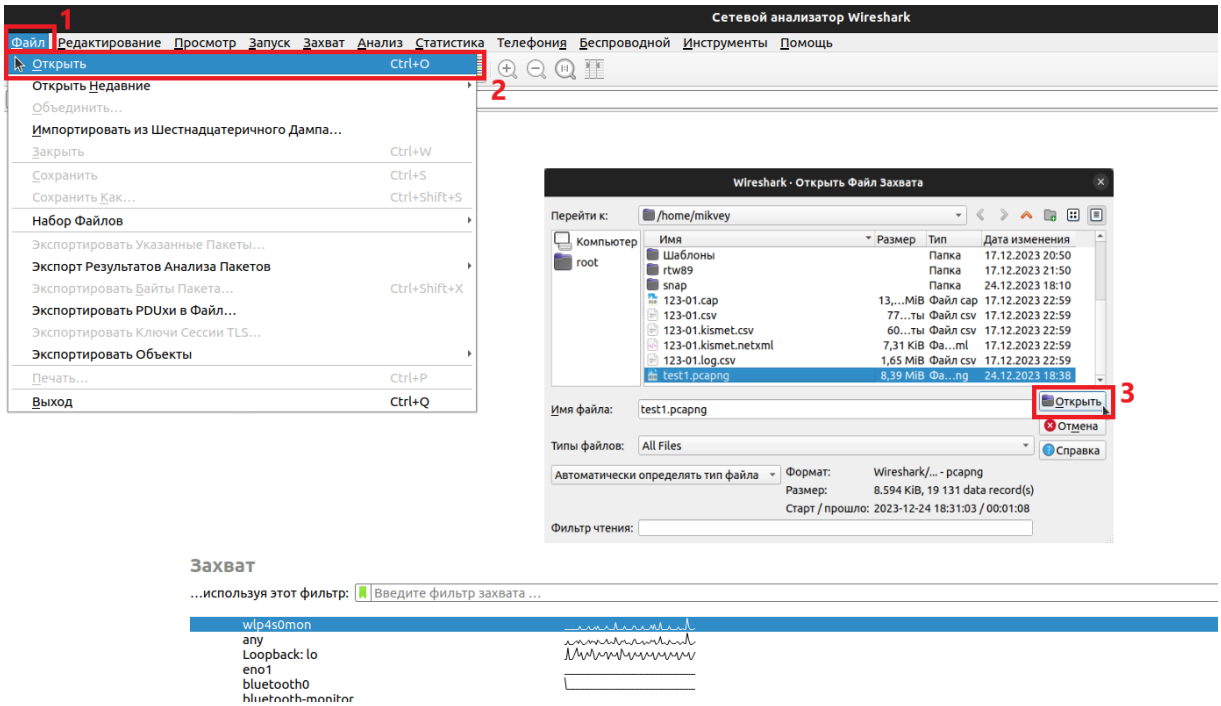

Рисунок 3.9 – Відкривання файлу перехоплених кадрів у Wireshark

І бачимо наступне (рисунок 3.10):

а) Панель фільтрів, котрі дозволяють знайти необхідну інформацію. Декілька фільтрів ми розглянемо згодом.

б) Панель найменувань, яка розділяє інформацію з пункту 3 на номери, час з початку захоплення трафіку, джерело та адресат, а також протокол, що використовувався, розмір пакету і невелику інформацію про мережевий пакет.

в) Панель пакетів, яка оновлюється в режимі реального часу. Але в нас вона статична, бо ми переглядаємо заздалегідь записаний файл. Тут інформація про пакети розділена по стовпчикам, які визначені на панелі найменувань.

г) Панель рівнів, які описують рівні моделі OSI обраного мережевого пакета.

д) Панель метаданих, яка представляє дані в шістнадцятирічному коді і символах.

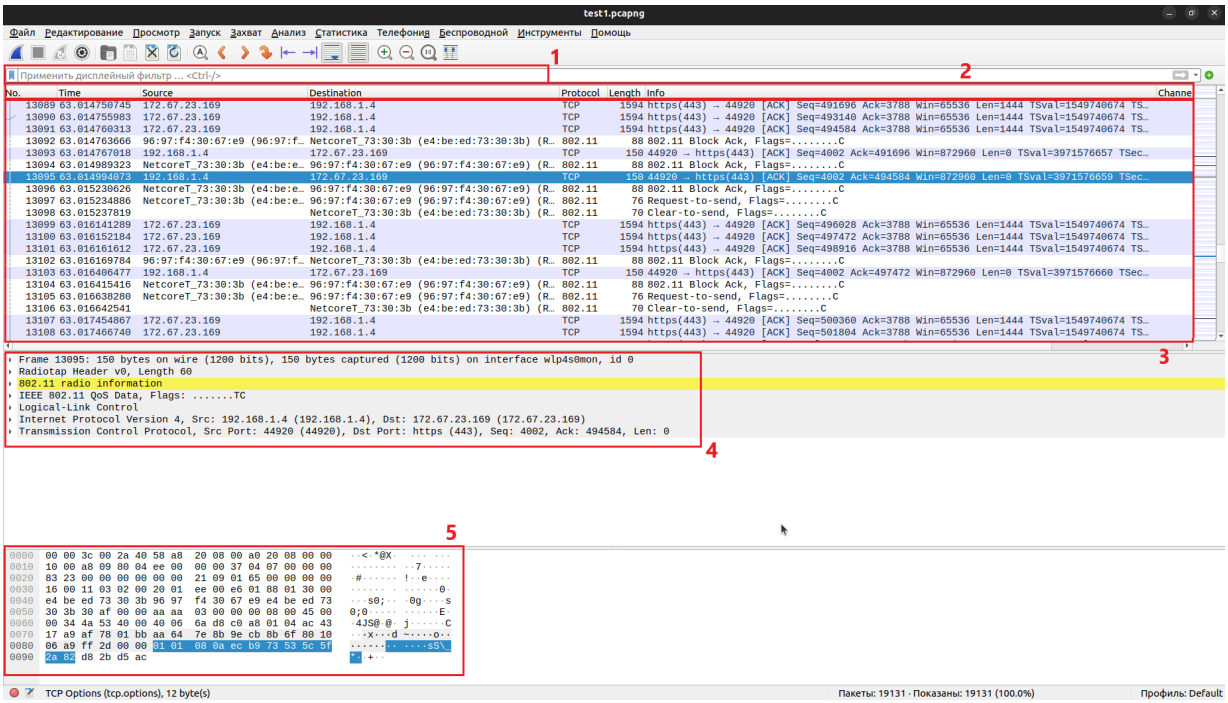

Рисунок 3.10 – Перегляд перехоплених кадрів у Wireshark

Під час захоплення трафіку в межах моніторингу бездротового адаптеру працювало дві Wi-Fi мережі, перша – наша тестова «testAP», друга – домашня мережа «Xiaomi_DDF3». Тож для зручності ми відфільтруємо трафік, щоб переглядати тільки той, що проходив через потрібну нам точку доступу. Так як ми знаємо MAC-адресу точки доступу, необхідний фільтр буде виглядати наступним чином – *wlan.bssid == E4:BE:ED:73:30:3B*.

А також давайте зразу переглянемо як саме пройшла аутентифікація при підключені нашого мобільного телефону до точки доступу. В цьому нам

допоможе ще один фільтр, який виглядає так - *wlan.fc.type_subtype == 11*. Об'єднаємо ці два фільтри за допомогою «&&», що означає логічне «І»:

wlan.bssid == E4:BE:ED:73:30:3 && wlan.fc.type_subtype == 11;

та дивимось результати (рисунок 3.11):

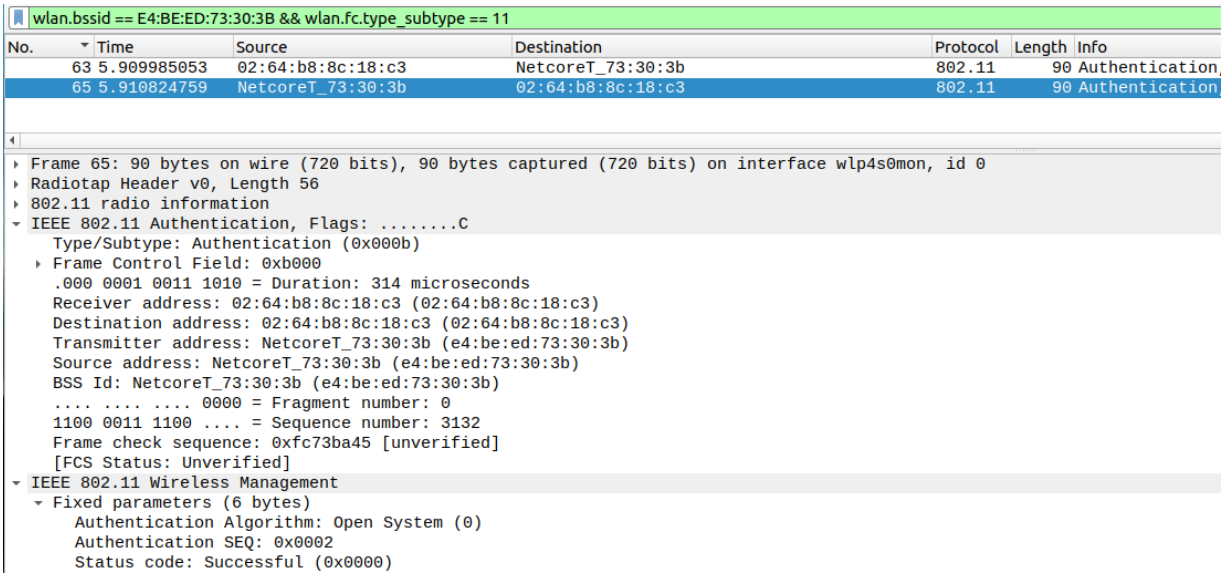

Рисунок 3.11 – Фільтрація трафіку по пакетам аутентифікації та MAC-адресі точки доступу

Так як наша Wi-Fi мережа абсолютно не захищена, використовувався метод відкритої аутентифікації (Open Authentication), так звана нульова аутентифікація. В процесі відкритої аутентифікації відбувається обмін двома повідомленнями:

а) станція, котра ініціювала процес аутентифікації, відправляє точці доступу кадр аутентифікації з номером послідовності 0x0001, який містить в собі запит аутентифікації;

б) точка доступу відповідає станції кадром аутентифікації з номером послідовності 0x0002

У випадку вдалої аутентифікації код стану в кадрі встановлюється в значення «успіх» (successful).

Ніякої реальної перевірки автентичності пристрою, який відправив запит на аутентифікацію, за допомогою цього механізму не здійснюється. Сторони просто обмінюються інформацією один про одного: клієнтський пристрій відправляє

запит, точка доступу відповідає на нього, після чого запускається процес асоціації. [2] Ці два кадри ми можемо спостерігати на рисунку 3.11.

Тож ніякого шифрування пакетів Wi-Fi у бездротовій мережі з відкритою аутентифікацією немає і наші пакети є абсолютно незахищеними для очей зловмисників. Давайте ж на них подивимось, прибираємо з поля фільтрів фільтр по пакетам аутентифікації та аналізуємо які ще пакети нам вдалось перехопити.

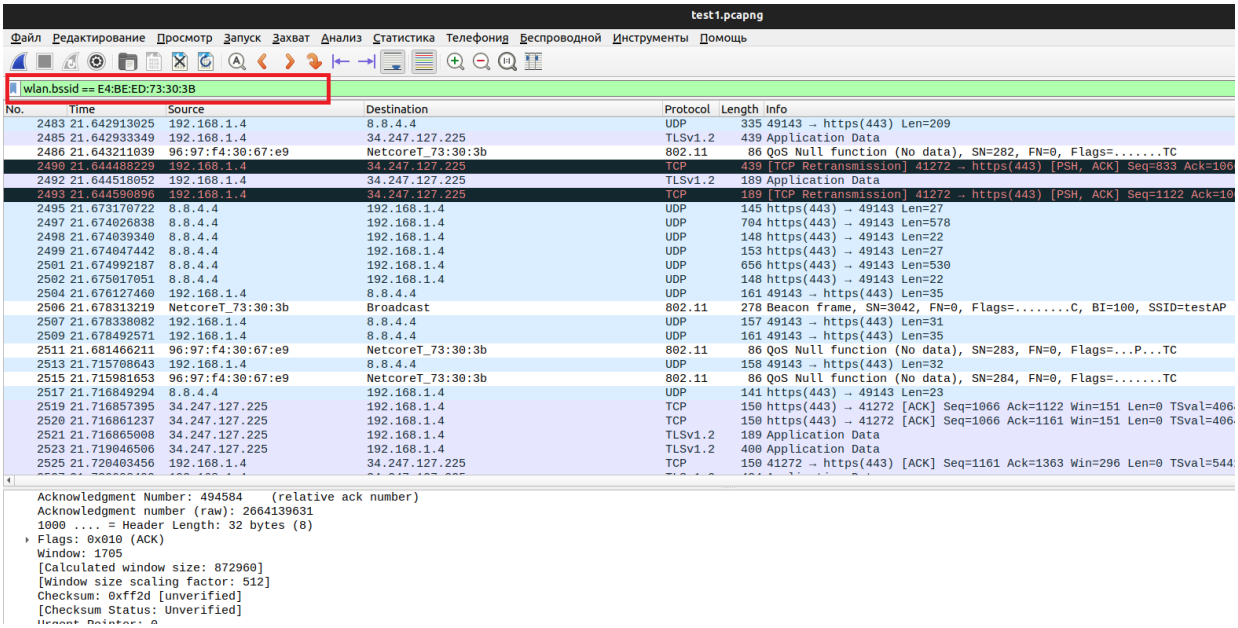

Рисунок 3.12 – Перехоплені пакети Wi-Fi

Перед нами знаходиться дуже багато інформації, якою можуть скористатись зловмисники в недоброзичливих цілях. Ми бачимо QUIC, TLS/TCP, SSL, HTTP/HTTPS, UDP, DNS, ARP та інші пакети. За допомогою цієї інформації можна дізнатись IP та MAC адреси підключених до точки доступу пристроїв, активність користувачів, відвідувані сайти, додатки та багато іншого.

Також, якщо користувач заходив на незахищені SSL сертифікатом сайти, тобто ті, що працюють на протоколі HTTP, ми можемо дізнатись персональні дані, логіни та паролі, користувача на цих сайтах. Давайте перевіримо, до нашого фільтру через «&&» додаємо ще один фільтр – «*http*»(1), і тепер ми бачимо пакети, що передані за протоколом HTTP(2). Тут є GET та POST запити до деякого сайту(3). Якщо ми відкриємо POST запит, після чого розгорнемо на

панелі рівнів OSI «HTML Form URL Encoded», ми побачимо логін та пароль, котрі користувач вводив на даному сайті. Це проілюстровано на рисунку 3.13.

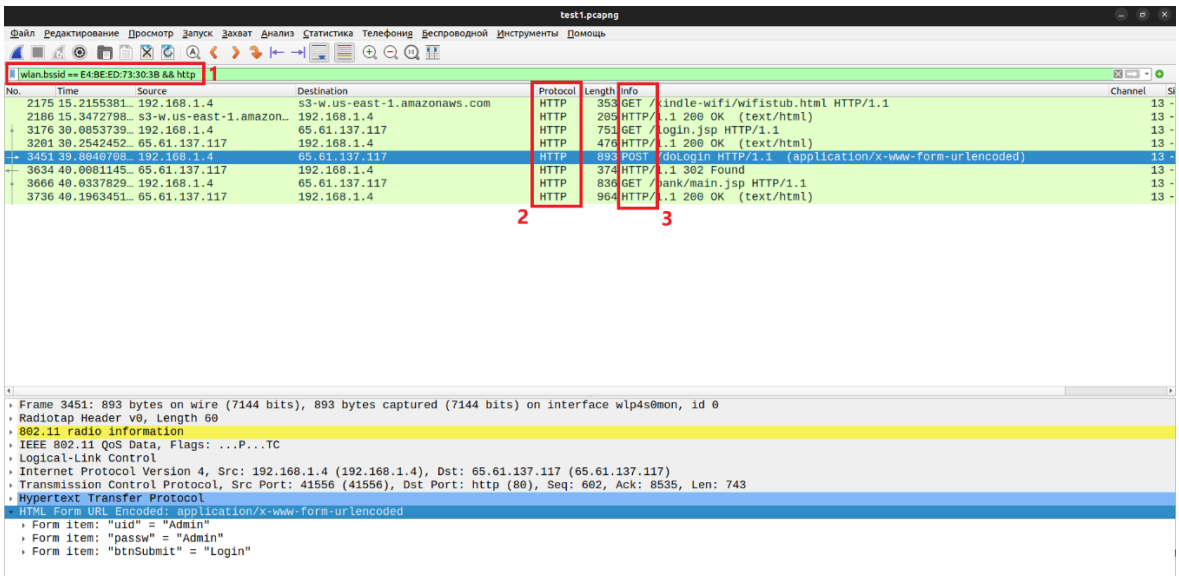

Рисунок 3.13 – Фільтрація пакетів за «http» та перегляд POST/GET-запитів між користувачем та веб-сайтом

Хоч і більшість теперішніх веб-сайтів працюють за протоколом HTTPS та мають шифрування запитів між користувачем та сервером, це не дає 100% гарантії не втратити ваші персональні дані через незахищеність мережі WI-Fi.

3.3.2 Аналіз зібраних даних досліду №2

Що ж, давайте тепер переглянемо як проходила аутентифікація між користувачем та точкою доступу в захищеній Wi-Fi мережі та як виглядають перехоплені нами кадри. Почнемо з аутентифікації, відкриваємо другий файл в Wireshark, відфільтровуємо за MAC-адресою точки доступу та додаємо сюди через || (логічне «або») відразу декілька фільтрів, а саме: *wlan.fc.type_subtype == 11, wlan.fc.type_subtype == 1, wlan.fc.type_subtype == 0* та *eapol.*

Наш фільтр виглядатиме наступним чином - *wlan.bssid == E4:BE:ED:73:30:3 && wlan.fc.type_subtype == 11 || wlan.fc.type_subtype == 1 || wlan.fc.type_subtype == 10 | eapol.* Подивимось на результат(рисунок 3.1X):

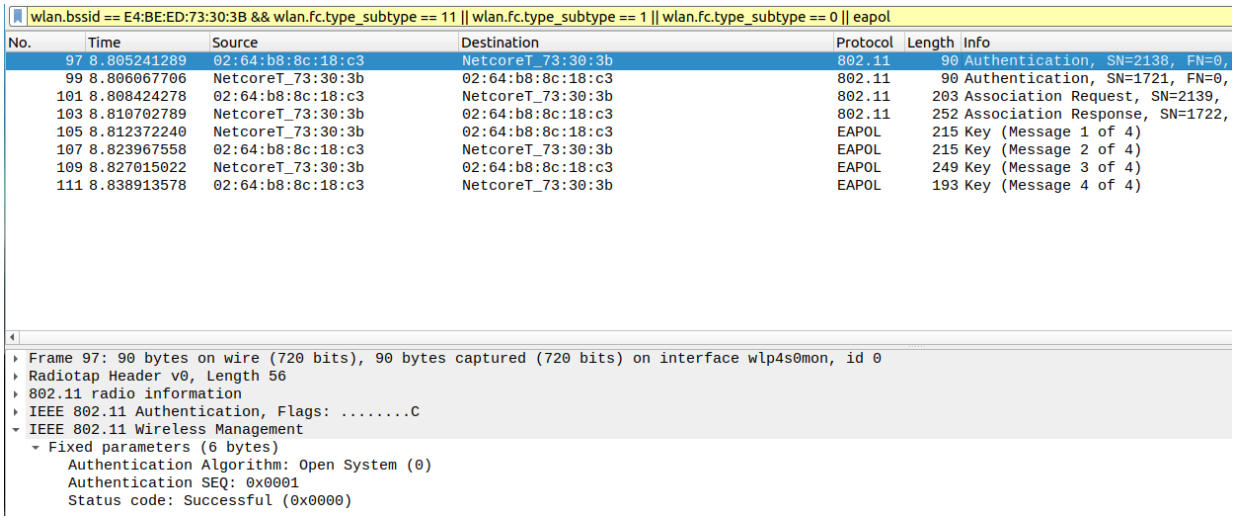

Рисунок 3.14 – Процес аутентифікації в захищеній WPA2 протоколом Wi-Fi мережі

Як ми можемо помітити на рисунку 3.14 порядок підключення користувача до точки доступу є наступним: Спочатку здійснюється відкрита аутентифікація та асоціація, після чого відбувається 4-етапне рукостискання (4-Way Handshake) пакетами EAPOL.

Відкрита аутентифікація виконується з метою забезпечення зворотної сумісності з машиною стану 802.11. Мета подальшої асоціації – узгодження набору можливостей забезпечення безпеки, які будуть використовуватись. Можливості забезпечення безпеки – це підтримувані протоколи конфіденційності і цілісності даних, методи аутентифікації і схеми управління ключами шифрування. Станція відправляю точці доступу запит на асоціацію, який містить перелік встановлених на ній параметрів безпеки. Якщо параметри безпеки точки доступу і станції не співпали, точка доступу відповідає відмовленням в асоціації. Якщо одержано позитивну відповідь на запит асоціації, станція перейде в третій стан «аутентифіковано та асоційовано» і почне процес 4-етапного рукостискання.

4-етапне рукостискання (4-way handshake) в протоколі WPA2 необхідне для аутентифікації клієнта та точки доступу один перед одним і створення

загального ключа шифрування для безпечної передачі даних між клієнтом і точкою доступу.

На кожному з 4 етапів відбувається наступне:

а) Точка доступу надсилає свій nonce (випадкове значення, що використовується лише один раз), а також параметри шифрування.

б) Клієнт надсилає свій nonce, параметри шифрування, MIC-код для перевірки цілісності, і підтверджує nonce від точки доступу.

в) Точка доступу перевіряє MIC-код повідомлення клієнта і надсилає свій MIC-код та підтвердження nonce клієнта.

г) Клієнт перевіряє MIC-код точки доступу.

Після успішного завершення 4-way handshake встановлюється захищене з'єднання за допомогою обміну ключами шифрування. На рисунку 3.15 більш детальніше показано перший з етапів 4-way handshake.

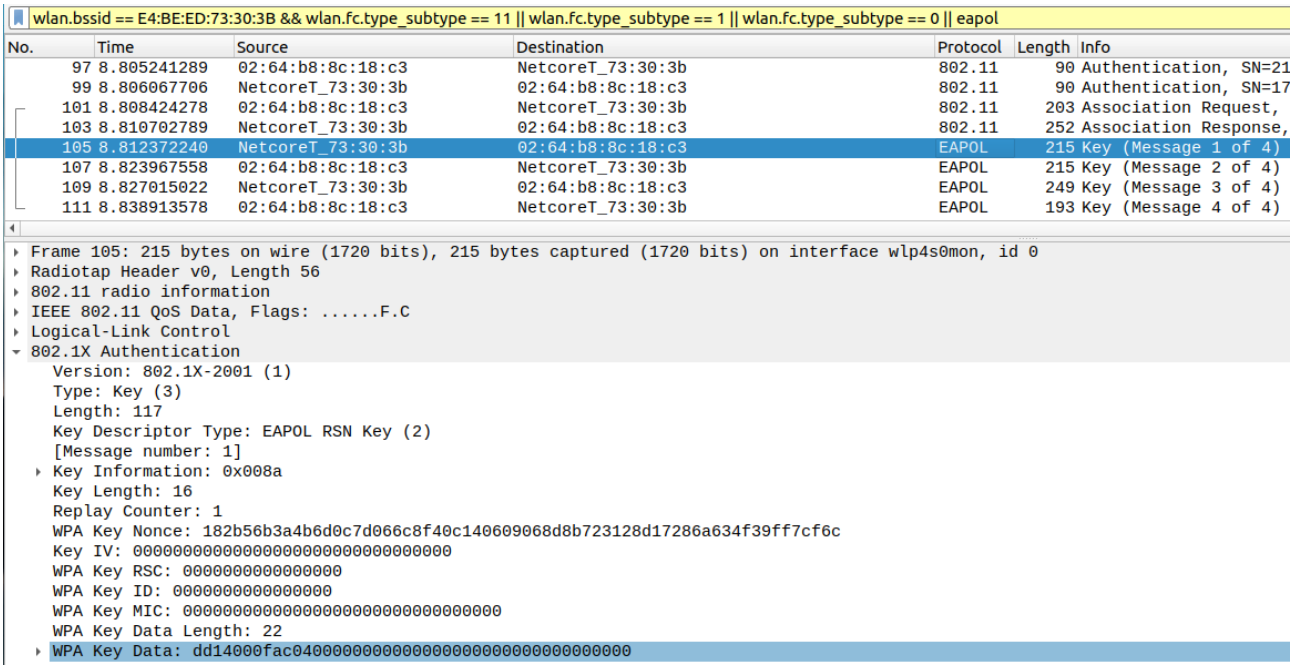

Рисунок 3.15 – Перший пакет EAPOL під час процесу 4-етапного рукостискання

А тепер давайте подивимось як виглядають перехоплені кадри в захищеній Wi-Fi мережі, прибираємо фільтри які були прописані до цього та залишаємо тільки фільтр за MAC-адресою. Бачимо наступні пакети (рисунок 3.16):

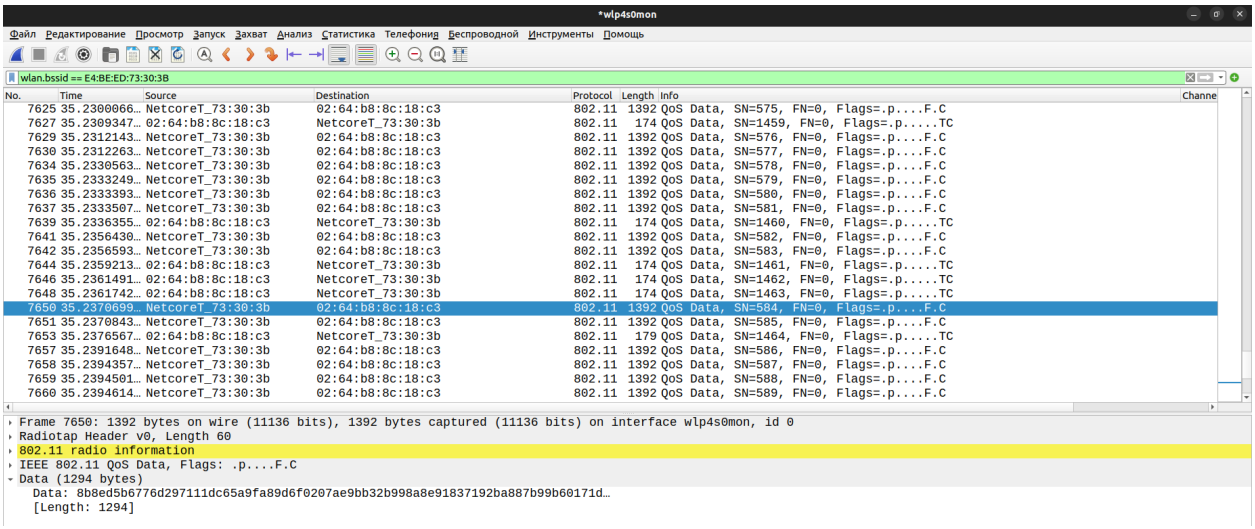

Рисунок 3.16 – Перегляд перехоплених кадрів в захищеній мережі Wi-Fi

Як ми можемо помітити абсолютно всі кадри зашифровані та не мають ніякої важливої інформації, яка могла б містити персональні дані користувача.

Тож після нашого аналізу можна з упевненістю сказати, що налаштування безпекових параметрів точки доступу є дуже важливим завданням в наш час і має велике значення для інформаційної захищеності користувачів.

3.4 Рекомендації щодо подальшого удосконалення та оптимізації налаштувань безпеки

В цьому пункті хотілось би визначити ключові аспекти захисту бездротових мереж Wi-F, засновані на проведених дослідженнях та аналізі трафіку. Результати експериментів виявили, що мережі без захисту стають вразливими перед несанкціонованим доступом, тимчасом як використання шифрування WPA2 значно ускладнює можливість перехоплення та використання трафіку.

Спостереження підтвердили, що без захисту всі дані, що пересилаються через мережу, легко доступні зловмисникам, використовуючи методи перехоплення пакетів. Захищена мережа WPA2, у свою чергу, надає ефективний захист від таких атак, оскільки шифрує трафік і ускладнює його інтерпретацію без необхідного ключа.

При рекомендаціях для підвищення безпеки Wi-Fi мережі, варто враховувати наступні аспекти:

а) **Використання сильного паролю**: Рекомендується встановлення надійних паролів, що складаються з комбінації букв, цифр та символів. Це значно ускладнить завдання зловмисникам при спробі злому.

б) **Широке впровадження шифрування WPA2/WPA3**: Використання сучасних протоколів шифрування є ефективним методом захисту від перехоплення трафіку та забезпечення конфіденційності.

в) **Ефективне управління доступом за допомогою MAC-адресної фільтрації**: Можливість обмеження доступу лише для конкретних пристроїв за їхніми MAC-адресами може стати ефективним шаром захисту.

г) **Регулярне оновлення паролів та ключів шифрування**: Зміна паролів та ключів з часом підвищить стійкість мережі, ускладнюючи можливість несанкціонованого доступу.

д) **Інформування та навчання користувачів**: Здійснюйте навчання персоналу та студентів про основи кібербезпеки та правила користування захищеною мережею.

Ці рекомендації допоможуть підвищити рівень безпеки Wi-Fi мережі та зменшити ризики, пов'язані із можливим несанкціонованим доступом та перехопленням трафіку.

3.5 Висновки

У цьому розділі дипломної роботи було проведено детальний аналіз механізмів захисту бездротових мереж Wi-Fi. Ubuntu Linux виступає як оптимальна операційна система для лабораторних умов, маючи штрокий набір інструментів та забезпечуючи високий рівень стабільності.

Інструменти, такі як aircrack-ng та Wireshark, надають студентам практичні навички з аудиту безпеки мережі та аналізу трафіку. Використання цих інструментів у лабораторних роботах покладає основи для ефективного управління та захисту бездротових мереж Wi-Fi у навчальних закладах.

4 РОЗРОБКА ЛАБОРАТОРНИХ РОБІТ ТА ТЕСТІВ ДЛЯ ПЕРЕВІРКИ ЗНАНЬ ЩОДО ЗАДАНОЇ ТЕМАТИКИ

4.1 Мета та завдання лабораторних робіт

Метою розробленого комплексу лабораторних робіт є надання практичних навичок студентам з налаштування параметрів безпеки та дослідження механізмів захисту в бездротових мережах Wi-Fi.

Виконання даних лабораторних робіт дозволить студентам не лише поглибити теоретичні знання в області безпеки Wi-Fi, але й застосувати їх на практиці під час конфігурації реального обладнання та аналізу процесів, що відбуваються в бездротовій мережі. Зміст лабораторних робіт знаходиться в додатку А (лабораторна робота 1) та додатку Б (лабораторна робота 2).

Нижче описані основні завдання, вирішення яких забезпечать запропоновані лабораторні роботи:

а) Ознайомлення з обладнанням бездротової мережі на практиці – робота з такими компонентами як точки доступу, адаптери, антени, кабелі. Це дасть студентам розуміння принципів функціонування апаратної складової Wi-Fi мереж.

б) Безпосереднє налаштування на обладнанні параметрів, які визначають безпеку бездротової мережі – режим роботи, типи аутентифікації, протоколи шифрування. Такі практичні навички є вкрай корисними для майбутніх фахівців в галузі інформаційної безпеки.

в) Дослідження процесів аутентифікації та асоціації бездротових клієнтів за допомогою спеціалізованих програм, таких як Wireshark. Це дасть студентам глибоке розуміння того, як відбувається підключення пристроїв до точки доступу, перевірка їх доступу та можливість почати передачу даних в мережі Wi-Fi. Аналіз реального трафіку є дуже цінним практичним досвідом.

г) Застосування різних методів та рекомендацій щодо посилення безпеки бездротової мережі – налаштування складних паролів, встановлення новітніх протоколів шифрування, обмеження доступу за MAC-адресами тощо. Практичне

оволодіння такими навичками суттєво підвищить рівень кібербезпеки на майбутніх робочих місцях випускників.

Отже, розроблений комплекс лабораторних робіт спрямований на комплексне вирішення задач навчання студентів безпеці бездротових мереж. Він охоплює як дослідження процесів, що відбуваються всередині Wi-Fi мереж (аутентифікація, асоціація, шифрування), так і практичну роботу по убезпеченню реальної мережі.

Лабораторні роботи передбачають використання як апаратних компонентів – точок доступу, адаптерів, антен, так і програмних – Wireshark, Aircrack-ng для аналізу трафіку.

Звіти з виконання робіт повинні містити детальний опис досліджуваних процесів, скріншоти налаштувань та результатів, висновки та рекомендації з вдосконалення захисту мережі.

Така практико-орієнтована підготовка дозволить випускникам відразу після закінчення ВНЗ застосовувати отримані навички захисту Wi-Fi мереж на робочому місці, ефективно виконуючи свої обов’язки в галузі інформаційної безпеки.

4.2 Зміст та опис лабораторних робіт

Розроблений комплекс містить 2 лабораторні роботи:

Лабораторна робота No1 - "Дотримання безпеки в бездротових мережах"

Лабораторна робота No2 - "Дослідження кадрів автентифікації стандарту IEEE 802.11"

Опис кожної з робіт:

Лабораторна робота No1

Мета: проаналізувати особливості роботи протоколів шифрування WEP та WPA2 в бездротовій мережі. Студенти зможуть на власному досвіді порівняти захищеність трафіку з використанням різних механізмів.

Обладнання та ПЗ: Робоча станція ПК1 з встановленим Wireshark, робочий девайс (ноутбук, телефон, ПК тощо) з функцією бездротового зв’язку Wi-Fi, Wi-Fi адаптер, точка доступу.

Порядок виконання:

а) Сконфігурувати лабораторне обладнання, налаштувати на точці доступу в режимі без шифрування.

б) Здійснити спробу перехоплення кадрів за допомогою Wireshark.

в) Повторити експеримент для протоколу WPA2 з використанням.

г) Порівняти можливість перегляду Wi-Fi трафіку в захищеній та незахищеній бездротових мережах Wi-Fi. Зробити висновки щодо їх захищеності.

Лабораторна робота No2

Мета: дослідити процеси аутентифікації та асоціації клієнтів у бездротовій мережі. Студенти на практиці зможуть побачити, як відбувається підключення пристроїв до точки доступу та отримання ними доступу до Wi-Fi мережі.

Обладнання та ПЗ: Робоча станція ПК1 з встановленим Wireshark, робочий девайс (ноутбук, телефон, ПК тощо) з функцією бездротового зв’язку Wi-Fi, Wi-Fi адаптер, точка доступу.

Порядок виконання:

а) Зібрати та налаштувати експериментальне обладнання.

б) За допомогою Wireshark "підслухати" процес аутентифікації новопід'єднаного клієнта. Проаналізувати послідовність обміну кадрами керування.

в) Дослідити вплив зміни параметрів безпеки на результат асоціації клієнта.

4.3 Методичні рекомендації до виконання робіт

Для успішного виконання запропонованих лабораторних робіт студентам слід дотримуватись наступних рекомендацій:

– Ретельно ознайомитись з теоретичним матеріалом з тем безпеки та захисту бездротових мереж. Це допоможе краще зрозуміти сутність практичних експериментів.

– Уважно прочитати методичні вказівки до кожної лабораторної роботи. Вони містять необхідну інформацію для успішного виконання.

– Суворо дотримуватись правил безпеки під час роботи з електрообладнанням.

– Складати звіт з кожної виконаної роботи з детальним описом усіх етапів, спостережень та висновків. Це закріпить отримані знання та навички.

Виконання цих рекомендацій допоможе студентам якісно та безпечно провести лабораторні дослідження механізмів захисту бездротових мереж.

Звіт з кожної лабораторної роботи має містити наступні обов'язкові пункти:

а) Мета роботи

б) Перелік використаного обладнання

в) Поетапний опис виконаних дій та спостережень

г) Скріншоти налаштувань, результатів аналізу трафіку

д) Висновки з проведеного дослідження

е) Відповіді на контрольні запитання в кінці роботи

Підготовка таких звітів закріпить у студентів розуміння процесів, які відбуваються всередині бездротової мережі під час аутентифікації та передачі даних. А також надасть практичні навички з убезпечення Wi-Fi.

4.4 Контроль набутих навичок та знань

Для оцінки якості засвоєння студентами матеріалу з безпеки Wi-Fi мереж після виконання лабораторних робіт, пропонується проводити наступні заходи контролю. Усне опитування безпосередньо під час виконання робіт. Студенти повинні пояснити викладачу принципи функціонування процесів, які вони досліджують у даний момент.

Також немало важливо є захист лабораторних звітів, коли дійснюється індивідуальна оцінку знань кожного студента на основі якості оформлення звіту і відповідей на запитання викладача.

В якості самоперевірки знань студентів були розроблені контрольні запитання, котрі розміщенні в кінці лабораторних робіт. Вони дозволять засвоїти знання та навички набуті в процесі виконання цих робіт, що покращить загальне сприйняття важливих знань безпеки бездротових мереж Wi-Fi.

Такий комплексний контроль надасть можливість якісно оцінити рівень оволодіння студентами лабораторного практикуму та вчасно виявити прогалини для їх коригування.

4.5 Висновки

Цей розділ дипломної роботи зосереджується на розробці лабораторних робіт для навчання безпеці бездротових мереж. Вивчаючи принципи функціонування Wi-Fi та виконуючи практичні завдання, студенти отримують не тільки теоретичні знання, але й практичні навички, які будуть корисні на майбутніх робочих місцях в сфері інформаційної безпеки. Контроль набутих навичок через захист звітів та усне опитування надає можливість оцінити якість засвоєння матеріалу та підготувати студентів до ефективного використання отриманих знань у практиці.

ВИСНОВКИ

У роботі було досліджено питання забезпечення безпеки бездротових мереж Wi-Fi та розроблено комплекс лабораторних робіт для навчання студентів принципам захисту таких мереж.

Було проаналізовано основні стандарти та механізми захисту Wi-Fi від несанкціонованого доступу та перехоплення трафіку. Досліджено можливості обладнання навчальних лабораторій щодо налаштування різних режимів безпеки.

За допомогою інструментів Wireshark та Aircrack-ng було проведено експерименти з перехоплення пакетів у тестовій Wi-Fi мережі та оцінено ефективність механізмів захисту.

На основі проведених досліджень було розроблено комплекс з 2 лабораторних робіт, спрямованих на вивчення студентами методів забезпечення безпеки бездротового зв'язку. До кожної роботи створено методичні вказівки та контрольні запитання.

Запропоновані лабораторні роботи дозволять студентам набути практичних навичок налаштування та тестування захисту Wi-Fi мереж, що сприятиме підготовці кваліфікованих фахівців з кібербезпеки.

Результати дослідження можуть бути використані для вдосконалення навчального процесу та підвищення рівня кіберзахисту на практиці. Роботу може бути продовжено в напрямку розробки інших лабораторних занять з актуальних питань мережевої безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лемешко А.В. Проектування безпроводових комп’ютерних мереж: навч. посібник / А.В. Лемешко, Л.А. Кирпач, Д.В. Сорокін, І.А. Бученко, М.М. Шрам. — К. : ДУТ, 2021. — 147 с.
2. Технологии современных беспроводных сетей : учебное пособие / [Е. В. Смирнова, А. В. Пролетарский и др.] ; под общ. ред. А. В. Пролетарского. – Москва : Издательство МГТУ им. Н. Э. Баумана, 2017. – 446, [2] с. : ил. – (Компьютерные системы и сети).
3. “Наука і сталий розвиток транспорту 2023”. Збірник тез доповідей Всеукраїнської науково-технічної конференції студентів і молодих учених М. Дніпро, УДУНТ, 2023- с. 141
4. Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості і освіті: Тези XVII Міжнародної науково-практичної конференції (Дніпро, 13-14 грудня 2023 р.). – Д.: УДУНТ, 2023. – 152 с.
5. Соколов В. Ю., Бурячок В. Л., Тадждіні М. М. Безпека безпроводових і мобільних мереж: навч. посіб. Київ: КУБГ, 2019. 130 с.
6. Чернега В., Платтнер Б. Безпровідні локальні комп’ютерні мережі: навч. посіб. Київ: Кондор, 2018. 238 с.
7. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам // Афанасьев А. А., Веденьев Л. Т., Воронцов А. А. – М.: Наука, 2012. - 552 с.
8. Мартинюк І.Є. Про один підхід до захисту інформації у wi-fi мережах стандарту 802.11 / І.Є. Мартинюк – Матеріали VII науково-технічної конференції «Інформаційні моделі, системи та технології» – Тернопіль, ТНТУ, 11-12 грудня 2019 р.– с. 68.
9. Комплексний підхід до захисту мовної інформації в технологіях безпровідного зв’язку / В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець, Р.І. Банах // Інформаційна безпека. – Східноукраїнський Національний університет імені Володимира Даля.) – 2013. – № 4(12). – С. 16-22

10. Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11 / Дмитро Мехед, Юлія Ткач, Володимир Базилевич, Тарас Петренко // Захист інформації, том 17, №4 – 2015 . – С. 285-291.
11. Рошан П., Лиэри Д. Основы построения беспроводных локальных сетей стандарта 802.11. – М.: Вильямс, 2004. — 304 с.
12. Wireshark. URL: https://www.wireshark.org/ (дата звернення: 17.10.2023).
13. Aircrack-ng. URL: https://www.aircrack-ng.org/ (дата звернення: 18.10.2023).
14. TP-Link. "N300 Wi-Fi роутер.". URL: https://www.tp-link.com/uk-ua/home-networking/wifi-router/tl-wr840n/ (дата звернення: 21.11.2023).
15. Netis. "Бездротовий маршрутизатор N серії.". URL: https://netis.ua/product/wf2419/ (дата звернення: 29.11.2023).
16. TP-Link. "TL-WR740N 150 Мбіт/с бездротовий маршрутизатор серії N.". URL: https://www.tp-link.com/uk-ua/home-networking/wifi-router/tl-wr740n/ (дата звернення: 17.10.2023).
17. D-Link. "Wireless N 150 PCI Adapter DWA-525." [Електронний ресурс] – Режим доступу: https://eu.dlink.com/uk/en/prodcts/dwa-525-wireless-n-150-pci-adapter (дата звернення: 01.12.2023).
18. D-Link. "Wireless AC1300 Dual-Band PoE Access Point.". URL: https://www.d-link.co.za/product/dap-2610/ (дата звернення: 13.11.2023).
19. Ubunt. URL: https://ubuntu.com/ (дата звернення: 28.11.2023).

ДОДАТОК А

Лабораторна робота №1.

ДОТРИМАННЯ БЕЗПЕКИ В БЕЗДРОТОВИХ МЕРЕЖАХ.

Мета роботи. Ознайомитися з принципами розгортання Wi-Fi мереж. Вивчити веб-інтерфейс налаштувань точки доступу, навчитися налаштовувати точку доступа. Засобами програми Acrylic Wi-Fi Analyzer дослідити створену та налаштовану мережу, проаналізувати її працездатність.

1.1 Загальні принципи захисту бездротових мереж

Бездротове середовище передачі даних є фізично загальнодоступним, тому потребує наявності сервісів автентифікації та конфіденційності даних. Стандарти та протоколи безпеки бездротових мереж визначені IEEE в рамках сімейства стандартів IEEE 802.11. Комерційні реалізації цих стандартів визначаються і сертифікуються Wi-Fi Alliance.

Стандарт IEEE 802.11-1999 визначив два методи автентифікації: автентифікацію відкритих систем та автентифікацію зі спільним ключем. Для забезпечення конфіденційності даних використовувався протокол WEP. У 2004 р. ратифіковано протокол IEEE 802.11i, фінальна версія якого отримала назву Robust Security Network (RSN) — мережа з посиленим режимом безпеки. У 802.11i визначено використання автентифікації на основі попередньо встановлених ключів (PSK) та автентифікації на основі стандарту IEEE 802.lX. Для забезпечення конфіденційності та цілісності даних використовуються протоколи TKIP та CCMP. Програми сертифікації WPA/WPA2 засновані на IEEE 802.11i та визначають набір функцій безпеки, які мають бути присутні у виробничому обладнанні для забезпечення безпеки бездротових мереж. Залежно від вимог мережі WPA/WAP2 працюють в одному з двох режимів — Enterprise або Personal. Режим Personal заснований на автентифікації PSK, режим Enterprise — на автентифікації на основі стандарту IEEE 802.lX. У WPA для забезпечення конфіденційності даних використовується протокол TKIP, в WPA2 — протокол CCMP.

Інформація про функції безпеки стандарту або точки доступу вказується в елементі RSN IE кадрів Beacon, Probe response, Association request.

У бездротових мережах можуть використовуватися механізми контролю доступу, що виходять за рамки стандарту IEEE 802.11. Контроль на підключення клієнта до точки доступу на основі його MAC-адреси не передбачений стандартами IEEE 802.11, проте підтримується багатьма виробниками обладнання для бездротових мереж, у тому числі D-Link. Для цього точка доступу повинна підтримувати функцію фільтрації за MAC-адресами (MAC

Filtering), яка дозволяє дозволяти або забороняти підключення клієнтів до мережі на основі їх MAC-адрес.

Мережевий адміністратор може налаштувати на точці доступу список дозволених або заборонених MAC-адрес. При спробі підключення бездротового клієнта точка доступу перевіряє заздалегідь налаштований список і визначає, чи дозволено цьому клієнту підключатися до мережі чи ні. Функція фільтрації за MAC-адресами може використовуватися спільно з механізмами автентифікації, наприклад відкритої автентифікації або автентифікації зі спільним ключем.

Необхідне обладнання (на 1 робоче місце):

- Робоча станція (ПК) ……..…… 1 шт.
- Девайс з Wi-Fi адаптером (телефон, ноутбук, ПК тощо)…… 1 шт.
- Мережевий адаптер D-Link DWA-525 ……. 1 шт.
- Точка доступу TL-WR740N …….. 1 шт.
- Кабель Ethetnet ……1 шт.
- ПЗ – аналізатор трафіку Wireshark.

1.2 Налаштування режиму WPA/WPA2-Personal

Перед виконанням завдання (рисунок 1.1) поверніть налаштування точки доступу до заводських налаштувань за замовчуванням. Для цього підключіть точку доступу до адаптера живлення і утримуйте кнопку Reset на задній панелі пристрою протягом 10 секунд (рис. 1.2).

Рисунок 1.1 – Схема мережі

Рисунок 1.2 – Кнопка Reset на точці доступу TL-WR740N

Підключіть Ethernet-кабель до LAN-порту точки доступу TL-WR740N та до мережевого адаптера робочої станції ПК1. Налаштуйте статичну IP-адресу 192.168.0.1 з маскою підмережі 255.255.255.0 на робочій станції ПК1.

Зайдіть у Web-інтерфейс точки доступу. Змініть IP-адресу управління на 192.168.N.50 з маскою підмережі 255.255.255.0. Збережіть і активуйте налаштування. Змініть IP-адресу Ethernet-адаптера робочої станції ПК1 на 192.168.N.1 з маскою підмережі 255.255.255.0. Зменшіть вихідну потужність передатчика точки доступу до 12,5%.

Створіть бездротову мережу з SSID class_N і налаштуйте режим захисту – Вимкнути захист (рисунок 1.3). Для цього:

1) Оберіть розділ Basic Settings ➔ Wireless;
2) В списку Mode оберіть Access Point;
3) В полі Network Name (SSID) введіть class_N;
4) Відключіть автоматичний вибір каналу. Для цього в полі Auto Channel Selection оберіть Disable;
5) В полі Channel оберіть 6;
6) У випадаючому меню Authentication оберіть Відключити захист;
7) збережіть налаштування, натиснувши кнопку Save.

Збережіть та активуйте налаштування. Для цього оберіть Configuration ➔ Save and Activate. Відключіть Ethernet-кабель від точки доступу. Налаштуйте на бездротових інтерфейсах ПК1 та робочого девайсу статичні IP-адреси у відповідності з рисунком 1.1.

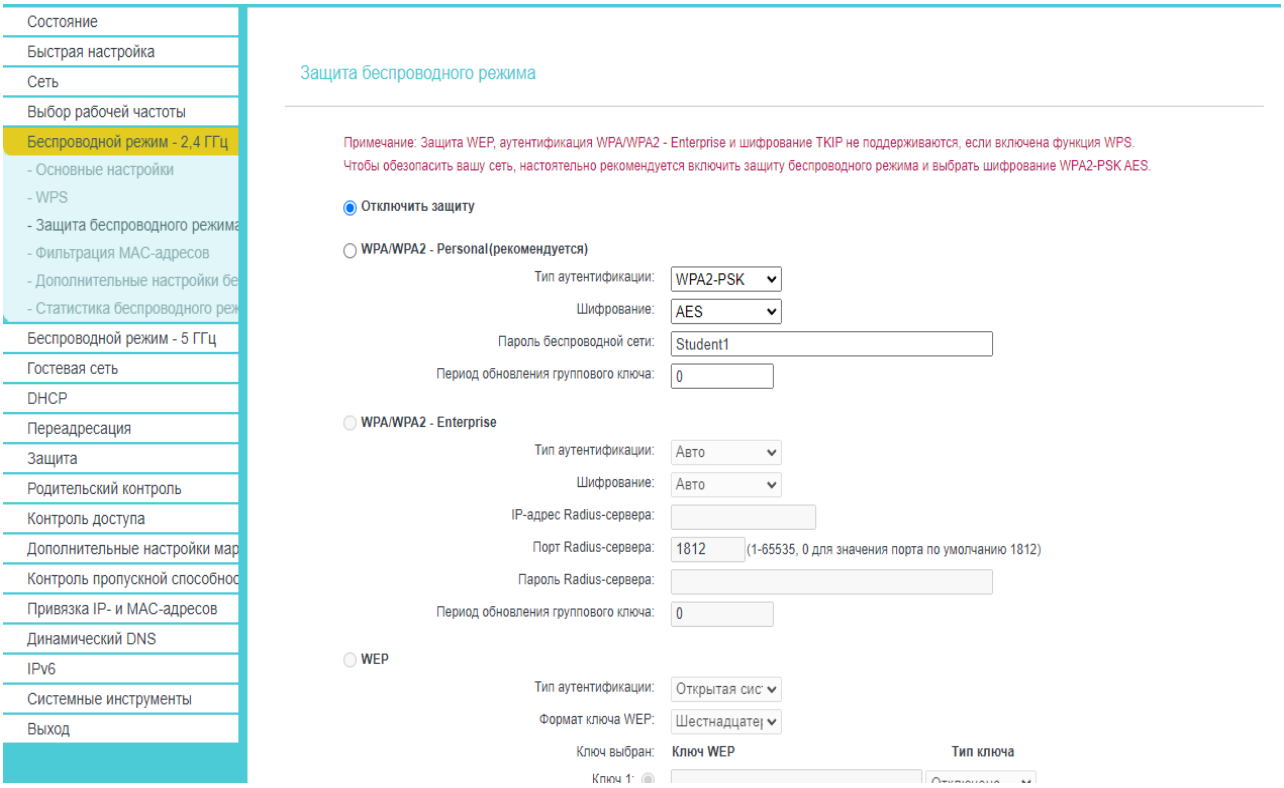

Рисунок 1.3 – Вікно налаштування точки доступу TL-WR740N

Запустіть на робочій станції ПК1 аналізатор протоколів Wireshark. Оберіть інтерфейс, з якого будете виконувати захоплення трафіку, і активуйте функцію моніторингу на бездротовому адаптері (рисунок 1.4).

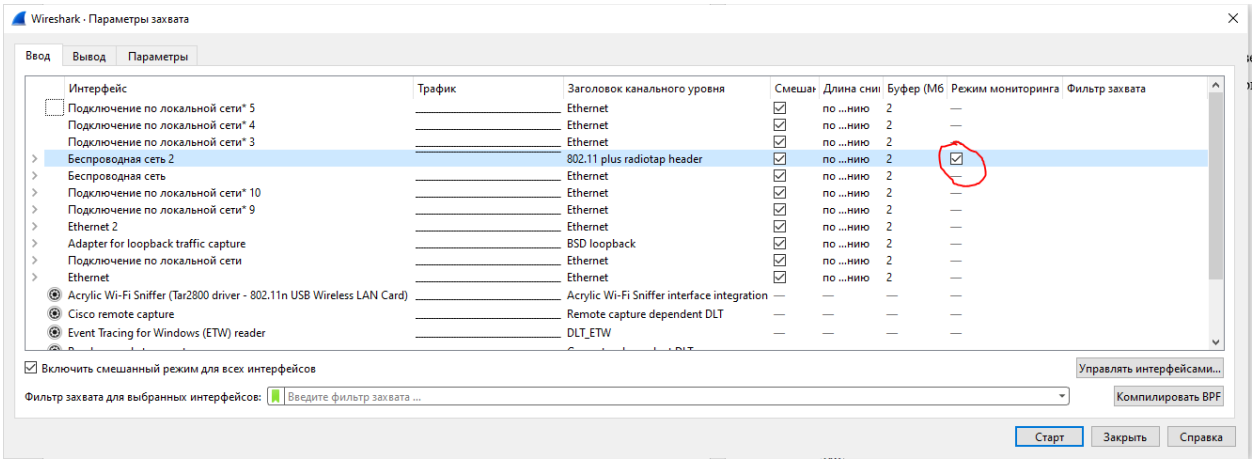

Рисунок 1.4 – Увімкнення режиму моніторингу бездротового адаптеру у Wireshark.

Запустіть процес захоплення трафіку. Для цього двічі натисніть на бездротовий адаптер з якого буде відбуватись захоплення та який переведено в

режим моніторингу. На робочому девайсі з можливістю підключення до Wi-Fi мережі (телефон, ноутбук, ПК тощо) під ’єднайтесь до бездротової мережі class_N. Із списку доступних бездротових мереж оберіть мережу з ідентифікатором class_N і натисніть кнопку Під ’єднатись та натисніть кнопку Ок.

На девайсі, з якого під ’єднались до точки доступу, виконайте різноманітні дії в браузері. Відкрийте будь-які сайти на свій розсуд. А також, для наочності передачі HTTP пакетів, перейдіть на сайт http://www.altoromutual.com/login.jsp та спробуйте ідентифікуватись з наступними даними: логін – Admin, пароль – Admin.

Зупиніть захоплення трафіку. Для цього натисніть кнопку Stop на панелі інструментів. Після чого проаналізуйте інформацію про передані кадри між точкою доступу та бездротовим клієнтом.

П р и м і т к а . В стовпчику Protocol ви бачите різні протоколи за якими передаються пакети Wi-Fi. Це можуть бути пакети QUIC, TLS/TCP, SSL, HTTP/HTTPS, UDP, DNS, ARP та інші.

Оберіть будь-який тип кадрів, який передавався між точкою доступу class_N та вашим девайсом. Для цього встановіть фільтр, наприклад, dns && Property.WiFiSSIDValue == “class_N”(замість «dns» ви можете встановити будь-який інший тип кадру). Натисніть кнопку Apply (рисунок 1.5).

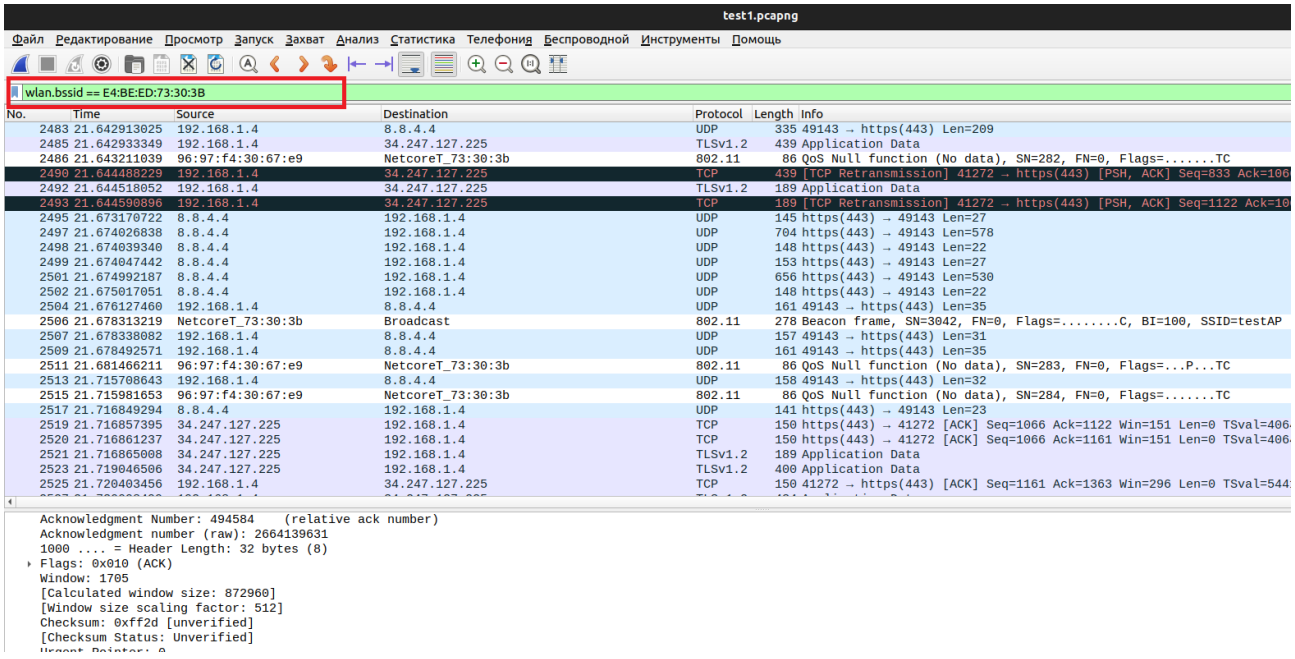

Рисунок 1.5 – Перехоплені кадри DNS

Проаналізуйте різні типи кадрів, змінюючи налаштування фільтру пошуку.

Які, на Вашу думку, важливі кадри може переглянути зловмисник в незахищеній мережі Wi-Fi?_____

В полі фільтрів вкажіть наступний фільтр - http && Property.WiFiSSIDValue == “class_N” для того, щоб переглянути пакети HTTP, якими ви обмінювались з веб-сайтом www.altoromutual.com. Проаналізуйте ці пакети. Тепер оберіть HTTP пакет з POST-запитом. Розгорніть «HTML Form URL Encoded» на панелі рівнів OSI (рисунок 1.6).

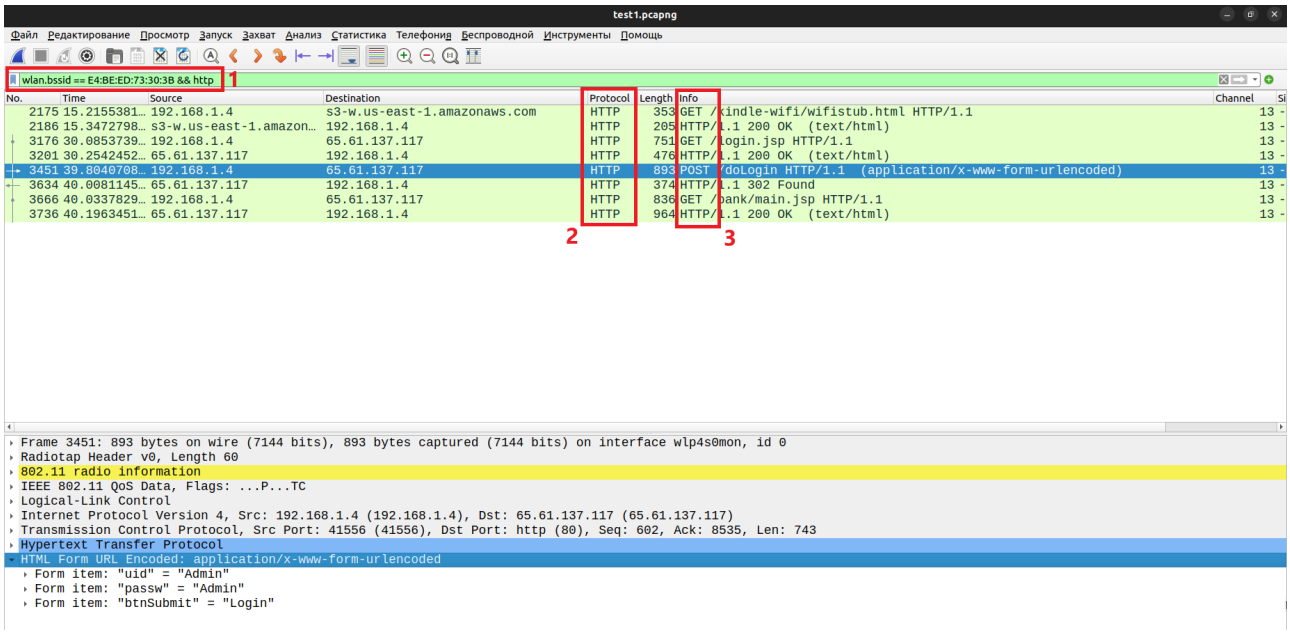

Рисунок 1.6 – Перегляд POST-запиту між користувачем і сайтом

Переконайтесь, що ви бачите логін та пароль за якими ідентифікувались на даному сайті. Від’єднайтесь від бездротової мережі class_N.

Змініть безпекові налаштування бездротової мережі class_N. Для цього зайдіть у Web-інтерфейс і налаштуйте режим WPA/WPA2-Personal:

1) Basic Settings ➔ Wireless;
2) У випадаючому меню Authentication оберіть WPA/WPA2-Personal;
3) В списку Тип аутентифікації оберіть WPA2-PSK;
4) В списку Шифрування оберіть AES;
5) В полі Пароль бездротової мережі введіть пароль Student1;
6) Збережіть налаштування, натиснувши кнопку Save.

Збережіть та активуйте налаштування. Для цього оберіть Configuration ➔ Save and Activate.

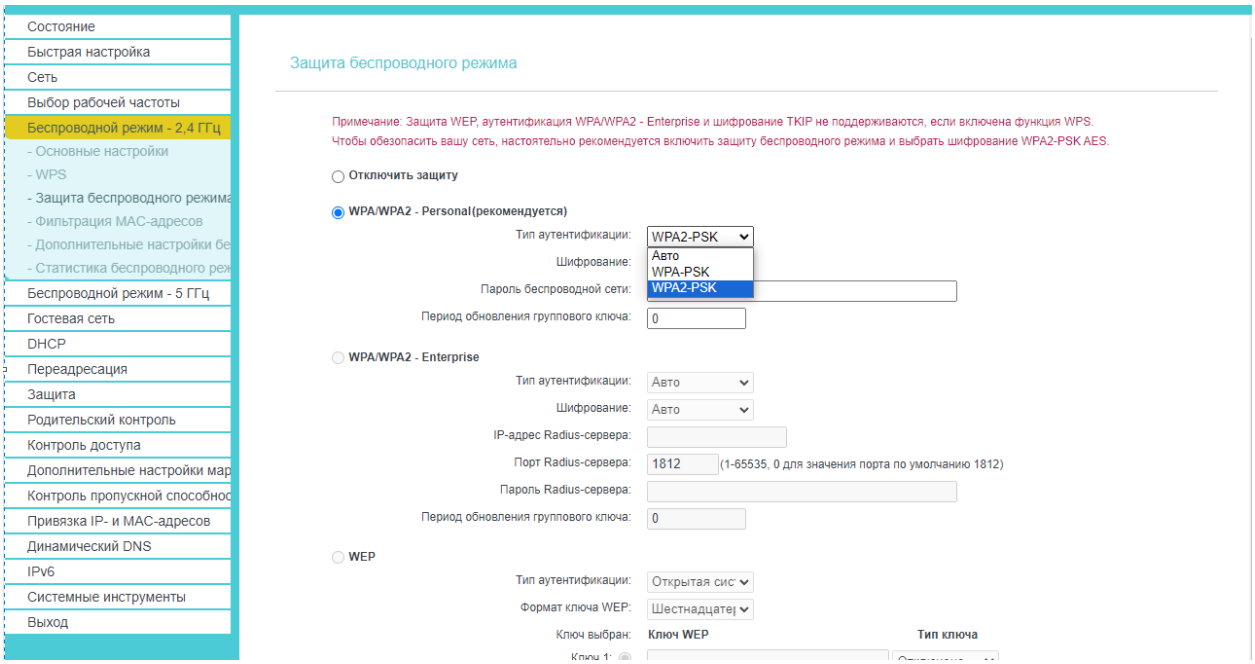

Рисунок 1.7 – Вікно налаштувань WPA/WPA2-Personal

Тепер повторіть кроки 10-14. Проаналізуйте кадри, які вдалось перехопити. Переконайтесь, що всі кадри які ви бачите, є зашифрованими та не містять конфіденційної інформації. Чи є такі кадри, якими могли б скористатись зловмисники, якщо є, то які? _____

1.3 Контроль доступу до бездротової мережі на основі MAC-адрес

Перегляньте MAC-адреси бездротових інтерфейсів ПК1 та вашого девайсу. Для того, щоб дізнатись MAC-адресу ПК – введіть в командному рядку наступну команду: getmac. Щоб дізнатись MAC-адресу телефону – розгорніть детальну інформацію в налаштуваннях бездротового з'єднання.

MAC-адреса ПК? _____

MAC-адреса вашого девайсу? _____

Під'єднайте робочу станцію ПК1 до дочки доступу Ethernet-кабелем. Зайдіть у Web-інтерфейс. Оберіть Advanced Settings ➔ Filters ➔ Wireless MAC ACL. Увімкніть фільтрацію підключень до точки доступу за MAC-адресами – в полі Access Control List виберіть Accept. В полі MAC Address введіть MAC-адресу вашого девайсу і натисніть кнопки Add та Save (рисунок 1.8).

Увімкнений фільтр діє по типу «білого списку»: асоціюватись з точкою доступу буде дозволено тільки пристроям, MAC-адреси котрих містяться у списку. Збережіть та активуйте налаштування. Від'єднайте Ethernet- кабель від точки доступу.

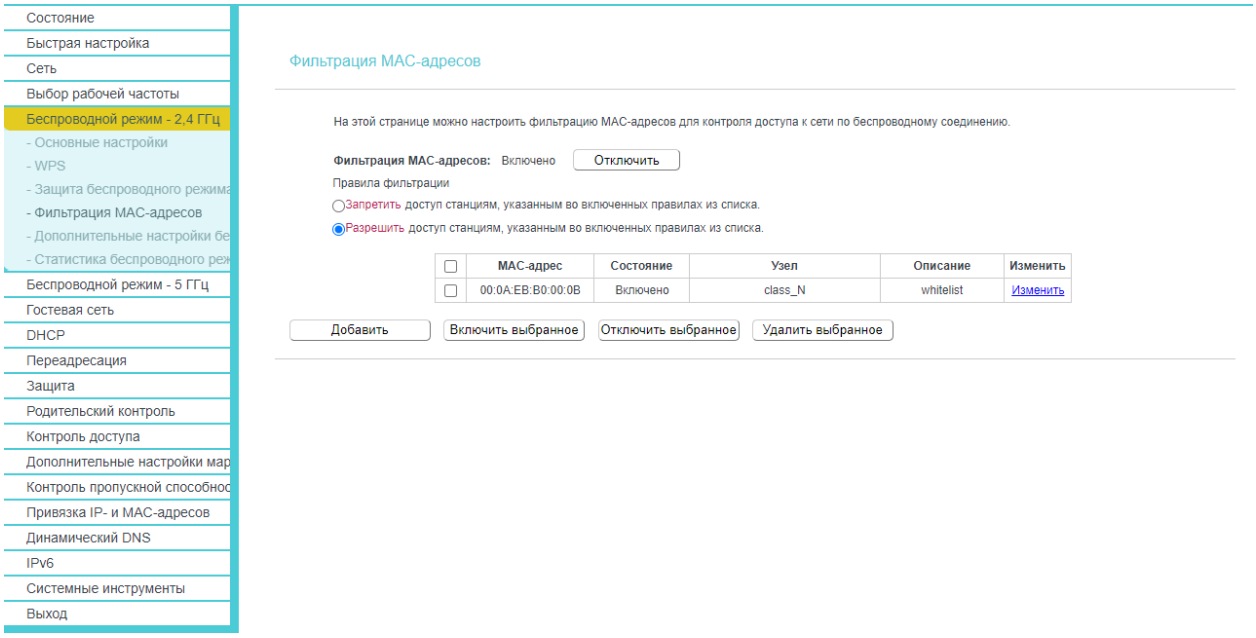

Рисунок 1.8 – Налаштування фільтрації за MAC-адресами по типу «білого списку»

Під ’єднайтесь на робочій станції ПК1 та вашому девайсі до бездротової мережі class_N.

Чи пройшла асоціація робочої станції ПК1 з точкою доступу? _____

Чи пройшла асоціація вашого девайсу з точкою доступу? _____

На робочій станції ПК1 зайдіть до Web-інтерфейсу точки доступу. Оберіть Advanced Settings ➔ Filters ➔ Wireless MAC ACL. Змініть фільтр на той, що забороняє – в полі Access Control List оберіть Reject і натисніть кнопку Save (рисунок 1.9).

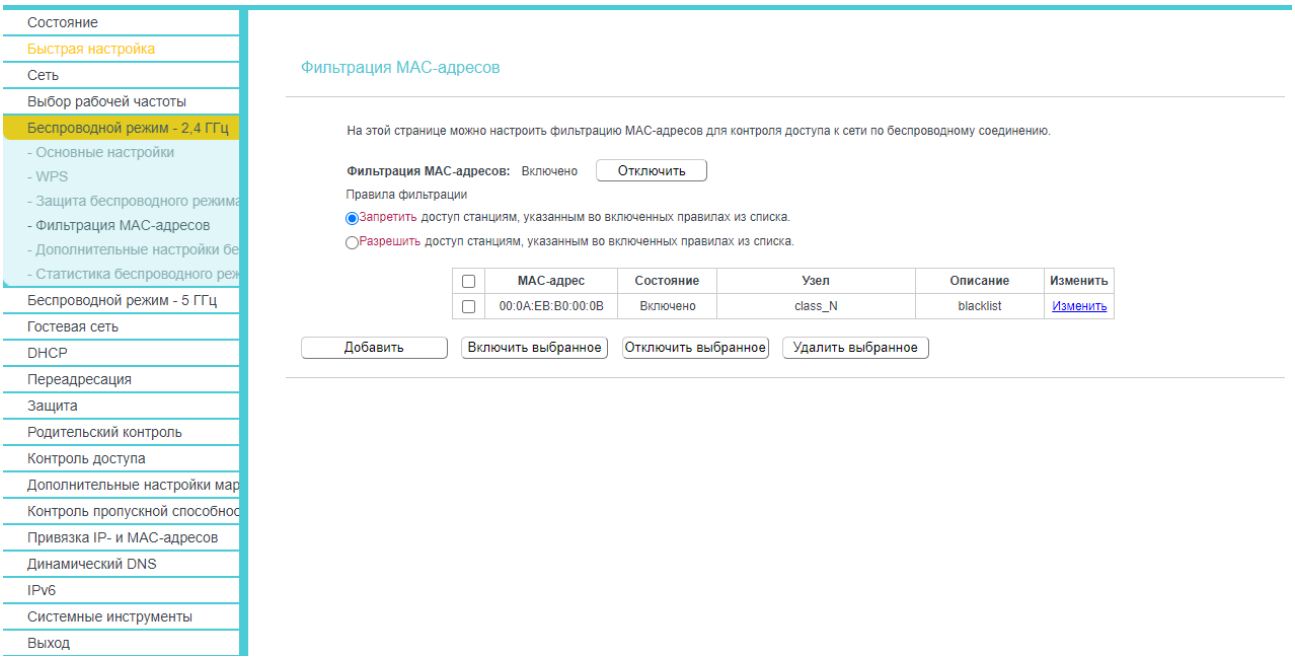

Рисунок 1.9 – Налаштування за MAC-адресами по типу «чорного списку».

Налаштований фільтр діє по типу «чорного списку»: асоціюватись з точкою доступу буде дозволено всім пристроям, окрім тих, чиї MAC-адреси містяться в списку. Збережіть і активуйте налаштування. Від'єднайте Ethernet-кабель від точки доступу.

Під 'єднайтесь на робочій станції ПК1 та вашому девайсі до бездротової мережі class_N.

Чи пройшла асоціація робочої станції ПК1 з точкою доступу? _____

Чи пройшла асоціація вашого девайсу з точкою доступу? _____

Відключіть фільтрацію підключень до точки доступу за MAC-адресами. Оберіть Advanced Settings ➔ Filters ➔ Wireless MAC ACL. В полі Access Control List оберіть Disable і натисніть кнопку Save. Збережіть і активуйте налаштування.

Під 'єднайтесь на робочій станції ПК1 та вашому девайсі до бездротової мережі class_N.

Чи пройшла асоціація робочої станції ПК1 з точкою доступу? _____

Чи пройшла асоціація вашого девайсу з точкою доступу? _____

1.4 Послідовність виконання роботи

1) До початку виконання лабораторної роботи ознайомтеся з загальними принципами захисту бездротових мереж Wi-Fi (п.1.1).

2) Налаштуйте Wi-Fi мережу відповідно до пункту 1.2

3) Встановіть та запустіть програму Wireshark, налаштуйте мережевий адаптер (п. 1.2)

4) Проведіть процес захоплення трафіку, після чого проаналізуйте захоплені кадри (п. 1.2)

5) Налаштуйте фільтрацію за MAC-адресою бездротових пристроїв (п.1.2)

6) Проаналізуйте роботу точки доступу в режимі фільтрації за MAC-адресами в «чорному» та «білому» списках

7) Оформіть звіт по роботі.

8) Пред'явіть звіт викладачеві і дайте відповідь на контрольні питання.

1.5 Зміст звіту

Звіт складається в електронному форматі і роздруковується. Звіт повинен містити:

- назву роботи;
- мету роботи;
- відповіді на поточні запитання;
- скріншоти налаштування мережі відповідно до наданого прикладу;
- скріншот інтерфейсу програми Wireshark;
- висновки до роботи.

1.6 Контрольні питання

1. Які основні протоколи та стандарти визначають безпеку бездротових мереж Wi-Fi?
2. Які існують основні методи аутентифікації в бездротових мережах?
3. Які протоколи забезпечують конфіденційність даних в бездротових мережах?
4. Які режими роботи підтримують протоколи WPA і WPA2?
5. Що таке фільтрація за MAC-адресами і як вона допомагає контролювати доступ до бездротової мережі?
6. Як перевести бездротовий адаптер в режим моніторингу в програмі Wireshark?
7. Які типи кадрів можна перехопити та проаналізувати за допомогою Wireshark в незахищеній мережі Wi-Fi?
8. Чи можна перехопити конфіденційну інформацію в захищеній мережі WPA2-PSK?
9. Яка різниця між "білим" та "чорним" списком MAC-адрес при фільтрації доступу до точки доступу?
10. Які переваги та недоліки має використання фільтрації за MAC-адресами для контролю доступу в бездротовій мережі?

ДОДАТОК Б

Лабораторна робота №2.

ДОСЛІДЖЕННЯ КАДРІВ АУТЕНТИФІКАЦІЇ СТАНДАРТУ IEEE 802.11

Мета роботи. Ознайомитися з програмою Wireshark для захвату та аналізу трафіку у Wi-Fi мережі. Вивчити інтерфейс програми, її основні функціональні можливості, отримати практичні навички по роботі з фільтрами. Засобами програми Wireshark дослідити Wi-Fi мережу.

2.1 Основні принципи автентифікації у відкритих та закритих бездротових мережах Wi-Fi

Розглянемо процес підключення бездротового клієнта до бездротової мережі, працюючої в інфраструктурному режимі. Для того, щоб бездротовий пристрій став повноцінним членом бездротової мережі, тобто асоціювався з точкою доступу, він має послідовно пройти через чотири стани.

Стан 1: початковий стан, не аутентифіковано, не асоційовано.

Стан 2: аутентифіковано, не асоційовано.

Стан 3: аутентифіковано і асоційовано (в очікуванні аутентифікації RSN).

Стан 4: аутентифіковано і асоційовано.

Діаграма станів показана на рисунку 2.1.

Для того, щоб бездротовий пристрій міг почати передачу даних через точку доступу, він має знаходитись в стані «аутентифіковано і асоційовано». Перехід в цей стан виконується поетапно шляхом обміну послідовностями кадрів керування 802.11.

Першою дією бездротового пристрою, який знаходиться в початковому стані, є виявлення бездротових мереж, в зоні дії яких він знаходиться. Клієнт відправляє фрейми пробного запиту (Probe Request). Точка доступу відповідає на пробний запит в тому випадку, якщо значення SSID (Service Set Identifier) співпадає з її особистим. Відповідь на пробний запит (Probe Response) містить інформацію про SSID, підтримці швидкостей передачі, типах шифрування і інших можливостей точки доступу. Він відправляється на індивідуальну адресу станції, яка відправила запит. Після того, як станція обрала точку доступу для підключення, вона відправляє їй запит на аутентифікацію.

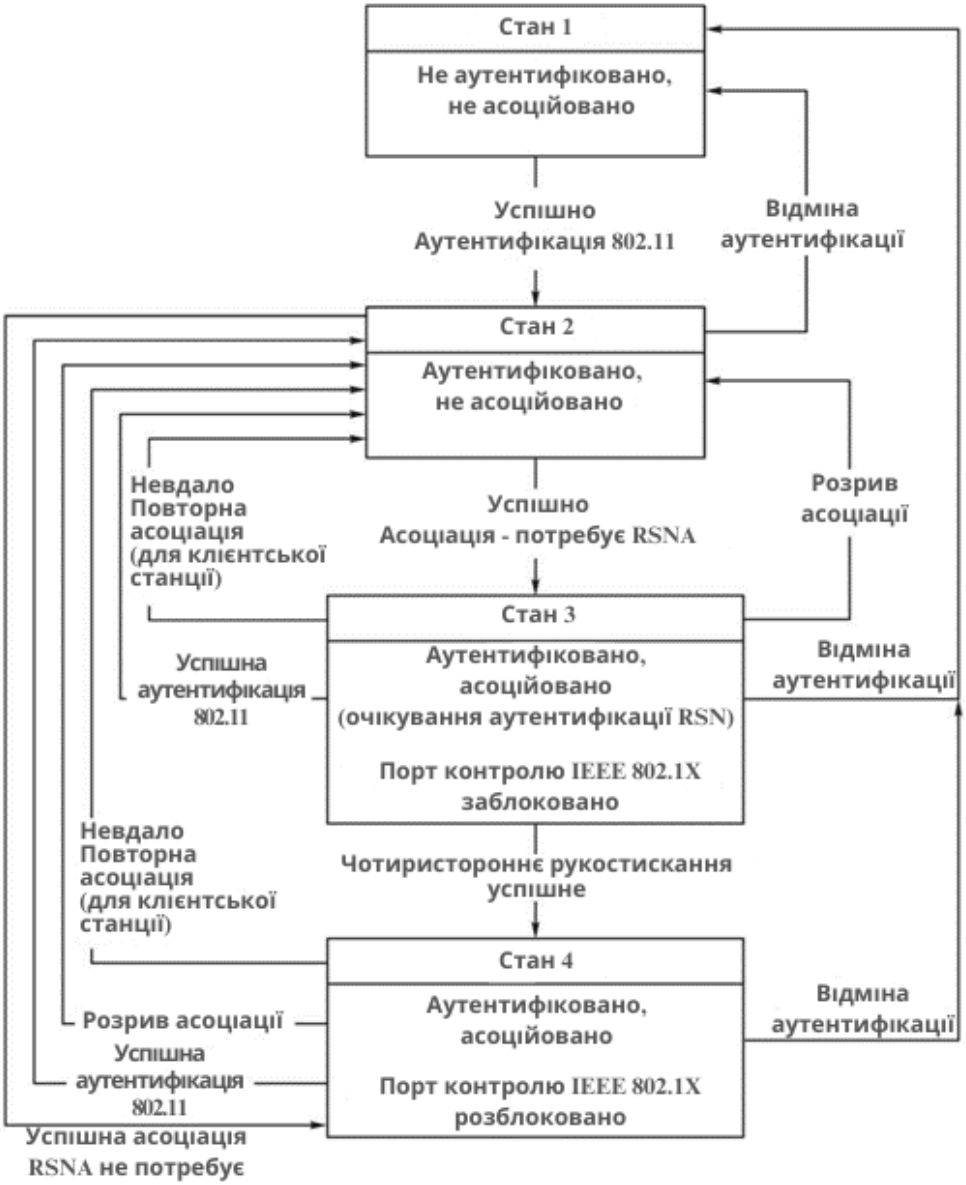

Рисунок 2.1 - Діаграма станів (машина станів) бездротового клієнта

В мережах IEEE 802.11 може використовуватись один з наступних типів аутентифікації:

- відкритих систем (Open System authentication);
- з загальним ключем (Shared Key authentication);
- з використанням паролю (Simultaneous Authentication of Equals, SAE);
- на основі стандарту IEEE 802.1X-2004;
- на основі попередньо встановлених ключів (Pre-Shared key, PSK).

Аутентифікація відкритих систем і аутентифікація з загальним ключем відносяться до методів аутентифікації мереж, попередніх мережам з посиленим

режимом безпеки (pre-RSN), тобто до методів, існуючих в оригінальному стандарті IEEE 802.11 (аутентифікація 802.11), маючого велику кількість вразливостей і не забезпечуючого аутентифікацію взаємодіючих приладів. У доповнення до методів безпеки, які існували в оригінальному стандарті, робоча група IEEE 802.11i розробила набір розширених функцій безпеки. В 2004 році стандарт IEEE 802.11i був ратифікований, і його фінальна форма отримала назву Robust Security Network (RSN) – мережу з посиленим режимом безпеки. Для надання послуг аутентифікації стандарт IEEE 802.11i опирається на IEEE 802.1X-2004 і механізм чотиристороннього рукостискання (4-Way Handshake), дозволяючи точкам доступу та бездротовим станціям безпечно обмінюватись ключами шифрування.

Для забезпечення конфіденційності і цілісності даних в стандарті визначені протоколи TKIP (Temporal Key Integrity Protocol) та CCMP (CTR with CBC-MAC Protocol). TKIP є необов'язковим і включений до стандарту для підтримки переходу з WEP на більш надійні протоколи. CCMP є обов'язковим для реалізації. Він заснований на алгоритмі шифрування AES (Advanced Encryption Standard) і більш стійкий до атак. В 2007 році стандарт IEEE 802.11i був включений в стандарт IEEE 802.11-2007.

А зараз розглянемо аутентифікацію на основі попередньо встановлених ключів, яка є найпоширенішим способом аутентифікації, що використовується в домашніх мережах та невеликих офісах. При аутентифікації на основі PSK на точці доступу і групі клієнтських станції, що підключаються до неї, потребується налаштування загального секрету, вид якого визначається ПЗ системи, що використовується. Секрет можна увести у виді строки з 64 шістнадцятирічних символів або у виді парольної фрази, що містить від 8 до 63 ASCII- символів. Для того, щоб створити ключ PSK довжиною 256 біти використовується спеціальна функція формування ключів, вхідними даними для якої є секрет, SSID мережі, в якій використовується цей секрет, довжина SSID, кількість ітерацій хешування і довжина ключа. Формування ключа PSK виконується до процесу обміну кадрами аутентифікації.

Почати процес аутентифікації може як точка доступу, так і станція, при цьому вони можуть зробити це одночасно.

Після того, як станція отримує інформацію про політику безпеки точки доступу з фрейму Beacon чи за допомогою активного сканування, сторони обмінюються двома фреймами аутентифікації 802.11 з номерами послідовностей 0x0001 та 0x0002, та відправляють один одному повідомлення Commit, в якому міститься ймовірний секретний ключ другої сторони. У відповідь на це повідомлення, якщо секретний ключ збігся, кожна зі сторін посилає повідомлення Confirm з підтвердженням.

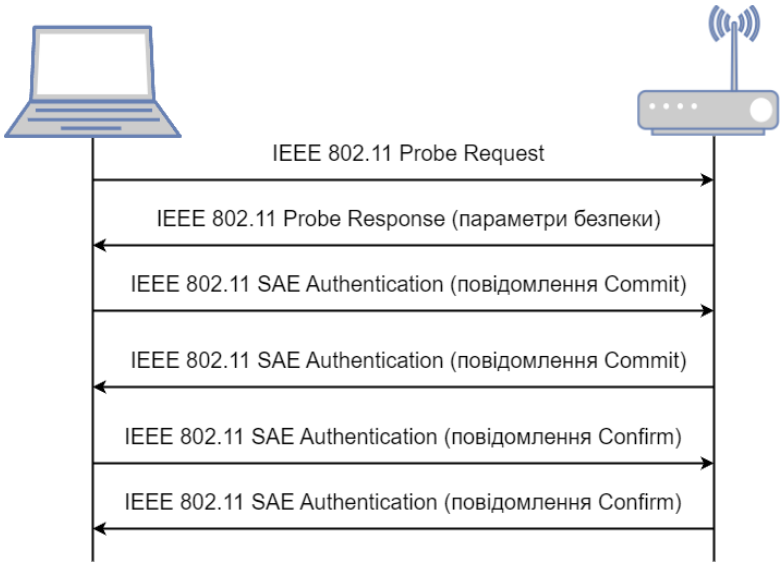

Рисунок 2.2 - Процес аутентифікації на основі PSK

Після успішної аутентифікації точка доступу і станція генерують із ключа PSK ключ PMK. Після чого станція асоціюється з точкою доступу і здійснюється домовленість про політику безпеки.

Згенерований в процесі аутентифікації ключ PMK використовується в процесі чотиристороннього рукостискання для генерації ключа PTK. Для шифрування і дешифрування широкомовного та групового трафіку точкою доступу генерується ключ GTK та додається на асоційованою з нею станцією. Після завершення цього процесу станція стає членом бездротової мережі і може почати безпечну передачу даних.

Необхідне обладнання (на 1 робоче місце):

- Робоча станція (ПК) ……..…… 1 шт.
- Девайс з Wi-Fi адаптером (телефон, ноутбук, ПК тощо)…… 1 шт.
- Мережевий адаптер D-Link DWA-525 ……. 1 шт.
- Точка доступу TL-WR740N …….. 1 шт.
- Кабель Ethetnet ……1 шт.
- ПЗ – аналізатор трафіку Wireshark.

2.2. Захоплення трафіку за допомогою мережевого аналізатора Wireshark

Перш ніж розпочати виконання завдання (див. рис. 2.3), поверніть налаштування точки доступу до заводських налаштувань за замовчуванням. Налаштування точки доступу виконується з робочої станції ПК 1.

Рисунок 2.3 – Мережева схема для пункту 4.1

Підключіть Ethernet-кабель до LAN-порту точки доступу та до Ethernet-адаптера робочої станції ПК 1. Далі налаштуйте статичну IP-адресу на Ethernet-адаптері робочої станції ПК 1 - 192.168.0.1 з маскою підмережі 255.255.255.0. Увійдіть до веб-інтерфейсу точки доступу. Змініть IP-адресу управління на 192.168.N.50 з маскою підмережі 255.255.255.0. Збережіть та активуйте налаштування. Змініть IP-адресу Ethernet-адаптера робочої станції ПК 1 на 192.168.N.1 з маскою підмережі 255.255.255.0.

Створіть бездротову мережу з SSID class_N і налаштуйте режим захисту – Вимкнути захист. Для цього:

8) Оберіть розділ Basic Settings ➔ Wireless;
9) В списку Mode оберіть Access Point;
10) В полі Network Name (SSID) введіть class_N;

11) Відключіть автоматичний вибір каналу. Для цього в полі Auto Channel Selection оберіть Disable;
12) В полі Channel оберіть 6;
13) У випадаючому меню Authentication оберіть Відключити захист;
14) збережіть налаштування, натиснувши кнопку Save.

Відключіть Ethernet-кабель від точки доступу. Налаштуйте статичні IP-адреси на бездротових інтерфейсах ПК 1 та ПК 2 у відповідності до рис. 2.3 та номером робочої групи. Запустіть на робочій станції ПК1 мережевий аналізатор Wireshark. Інтерфейс програми показано на рис 2.4.

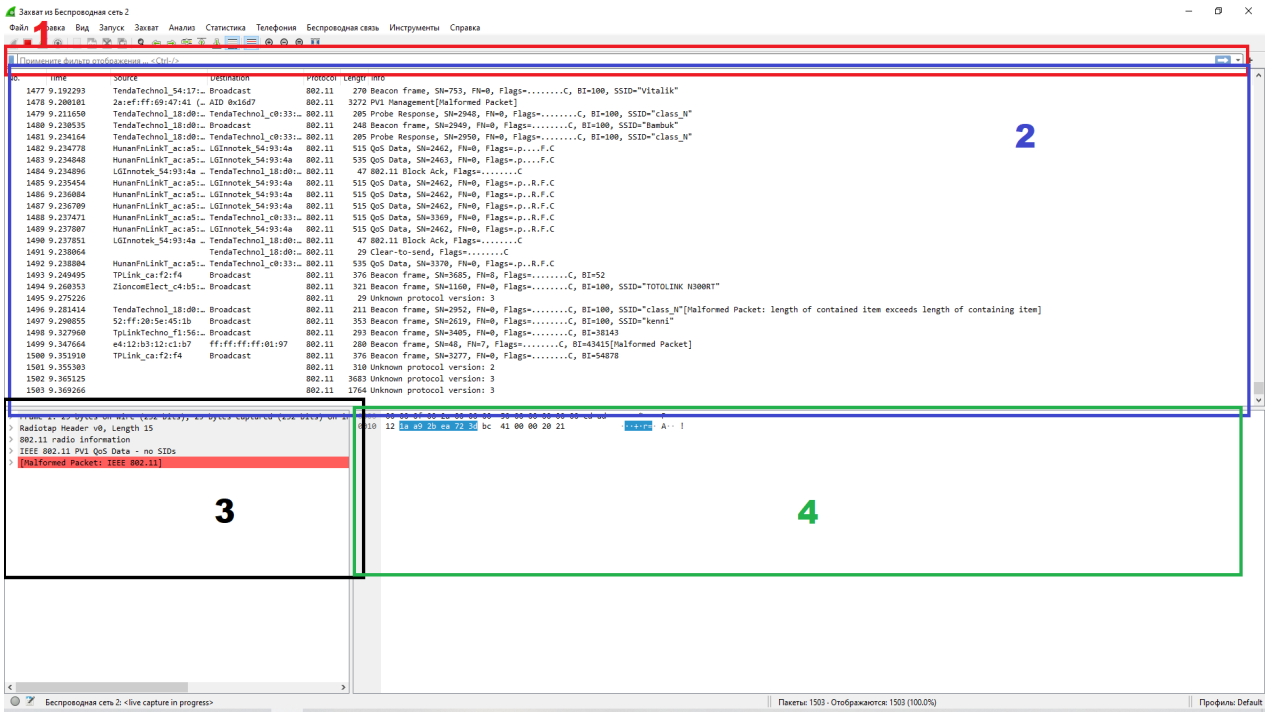

Рисунок 2.4 – Інтерфейс Wireshark

Інтерфейс **Wireshark** складається з кількох вікон. У вікні 1 ви можете створювати фільтри, що дозволяють вибирати певні кадри для їх аналізу. У вікні 2 міститься список всіх захоплених кадрів, організований у вигляді таблиці з заголовками. Виділяючи рядок таблиці, можна переглянути більш детальну інформацію про кадр та його розшифрування у вікні 3. Вікно 4 містить код кадру у шістнадцятковому та текстовому представленні.

Оберіть інтерфейс, з якого буде проводитися захоплення трафіку, та активуйте функцію моніторингу на бездротовому адаптері. Для цього натисніть кнопку налаштувань на панелі інструментів (рис. 2.5).

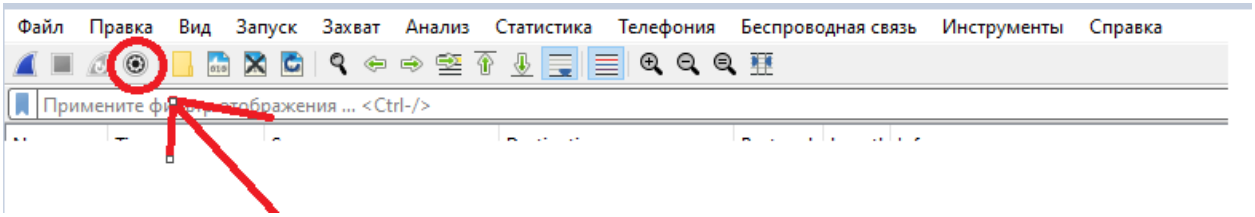

Рисунок 2.5 – Налаштування бездротового адаптера для захоплення трафіку

У відкритому вікні оберіть наш адаптер, та встановіть прапорець у колонці Режим моніторингу (рис. 2.6).

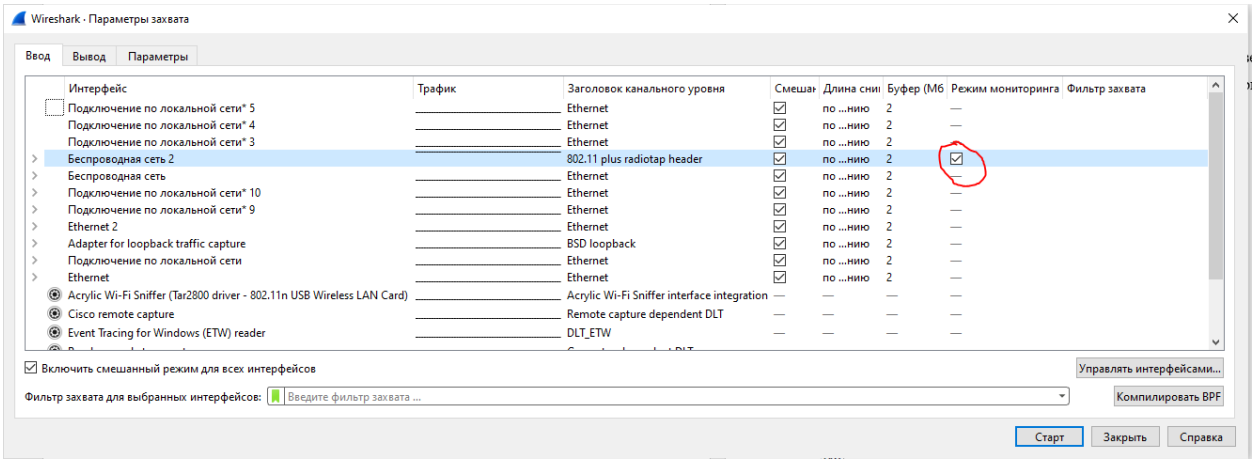

Рисунок 2.6 – Налаштування бездротового адаптера в режимі моніторингу.

Запустіть процес захоплення трафіку, натиснувши кнопку Почати захоплення трафіку на панелі інструментів (рис. 2.7).

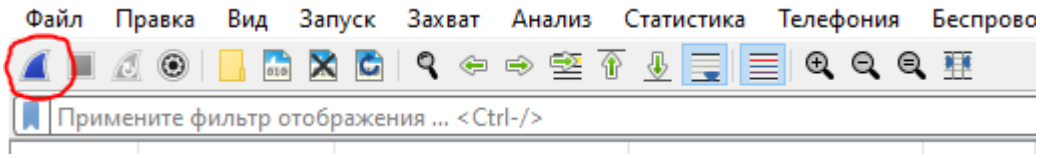

Рисунок 2.7 – Кнопка початку захоплення трафіку

На робочому девайсі з можливістю підключення до Wi-Fi мережі (телефон, ноутбук, ПК тощо) під ’єднайтесь до бездротової мережі class_N. Із списку доступних бездротових мереж оберіть мережу з ідентифікатором class_N і натисніть кнопку Під ’єднатись та натисніть кнопку Ок.

Зупиніть процес захоплення трафіку, натиснувши кнопку "Stop" на панелі інструментів. Від’єднайтесь від бездротової мережі class_N. Збережіть захоплені

кадри у файл. Для цього виберіть меню File ➔ Save As. У цьому вікні введіть ім'я файлу та натисніть кнопку Зберегти.

Змініть безпекові налаштування бездротової мережі class_N. Для цього зайдіть у Web-інтерфейс і налаштуйте режим WPA/WPA2-Personal. Після чого збережіть та активуйте налаштування. Для цього оберіть Configuration ➔ Save and Activate.

7) Basic Settings ➔ Wireless;
8) У випадаючому меню Authentication оберіть WPA/WPA2-Personal;
9) В списку Тип аутентифікації оберіть WPA2-PSK;
10) В списку Шифрування оберіть AES;
11) В полі Пароль бездротової мережі введіть пароль Student1;
12) Збережіть налаштування, натиснувши кнопку Save.

Запустіть процес захоплення трафіку, натиснувши кнопку Почати захоплення трафіку на панелі інструментів На робочому девайсі з можливістю підключення до Wi-Fi мережі (телефон, ноутбук, ПК тощо) під ’єднайтесь до бездротової мережі class_N. Із списку доступних бездротових мереж оберіть мережу з ідентифікатором class_N і натисніть кнопку Під ’єднатись, уведіть раніше заданий пароль та натисніть кнопку Ок. Зупиніть процес захоплення трафіку, натиснувши кнопку "Stop" на панелі інструментів. Від’єднайтесь від бездротової мережі class_N. Збережіть захоплені кадри у файл. Для цього виберіть меню File ➔ Save As. У цьому вікні введіть ім'я файлу та натисніть кнопку Зберегти.

2.3 Аналіз кадрів аутентифікації стандарту IEEE 802.11

Відкрийте перший збережений файл з захопленими кадрами у незахищеній бездротовій мережі. Для цього виберіть меню File ➔ Open.

У полі фільтрів встановіть фільтра для відображення лише кадрів автентифікації. Для цього введіть наступне - *wlan.fc.type_subtype == 11*. (рисунок 2.8). Після чого розгорніть IEEE 802.11 Wireless Management ➔ Fixed parameters на панелі рівнів OSI.

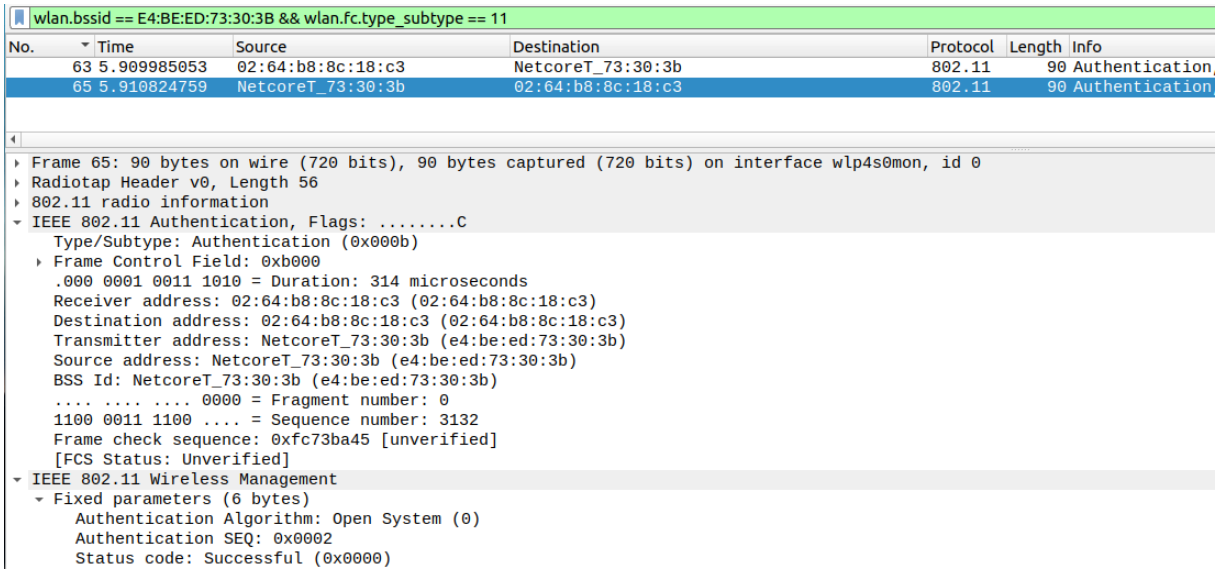

Рисунок 2.8 – Фільтрація трафіку по пакетам аутентифікації.

Проаналізуйте кадри аутентифікації (Authentication frames). Чи бачите ви весь діалог між точкою доступу та користувачем в процесі аутентифікації?_____ Скільки пакетів для цього знадобилось?_____ Який тип аутентифікації ви можете визначити з цих даних? _____

Закрийте цей файл. Для цього виберіть меню File ➔ Close. Тепер відкрийте другий збережений файл з захопленими кадрами у захищеній WPA/WPa-Personal бездротовій мережі. Для цього виберіть меню File ➔ Open.

У полі фільтрів встановіть фільтра для відображення лише кадрів автентифікації та кадрів 4-етапного рукостискання (eapol) між точкою доступу та бездротовим клієнтом. Для цього введіть наступне - *wlan.fc.type_subtype == 11 && eapol* («&&» виступає в якості логічного «І»). (рисунок 2.9).

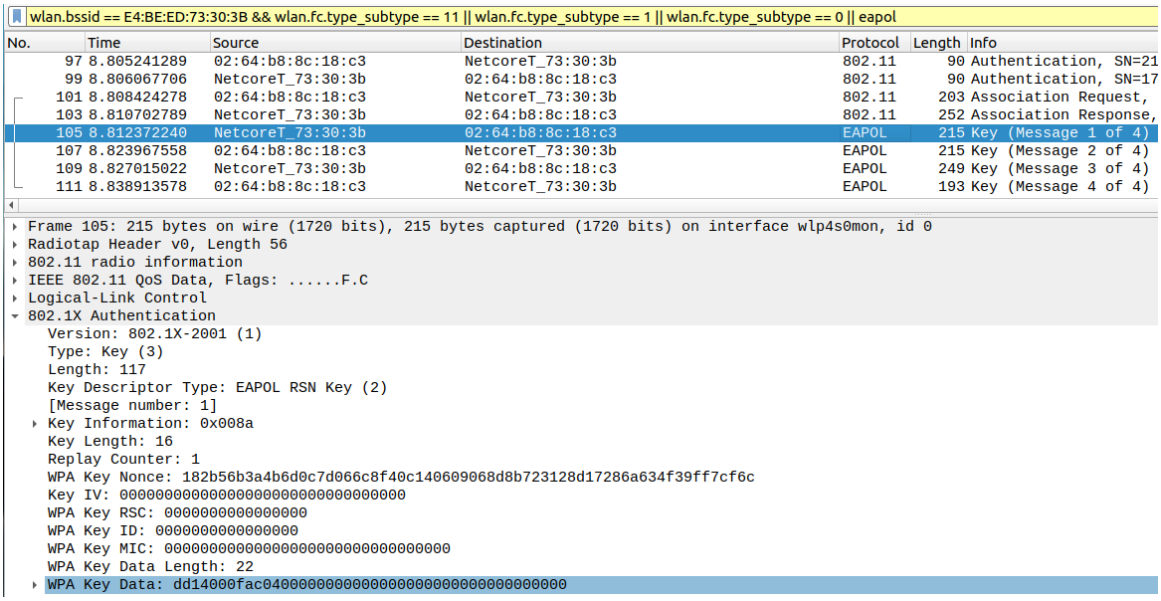

Рисунок 2.9 – Процес аутентифікації в захищеній WPA2 протоколом Wi-Fi мережі

Розгорніть IEEE 802.11 Wireless Management ➔ Fixed parameters на панелі рівнів OSI. Проаналізуйте кадри аутентифікації (Authentication frames) в захищеній Wi-Fi мережі. Чи бачите ви весь діалог між точкою доступу та користувачем в процесі аутентифікації?_____ Скільки пакетів для цього знадобилось?_____ Який тип аутентифікації ви можете визначити з цих даних? _____

2.4 Послідовність виконання роботи

1) До початку виконання лабораторної роботи ознайомтеся з основними автентифікації стандарту IEEE 802.11 (п.2.1).

2) Налаштуйте Wi-Fi мережу (п.2.2)

3) Встановіть та запустіть програму Wireshark, налаштуйте мережевий адаптер (п.2.2)

4) Проведіть процес захоплення трафіку, та збережіть його у файл (п.2.2)

5) Проаналізуйте захоплені кадри аутентифікації (п.2.3).

6) Оформіть звіт по роботі.

7) Пред'явіть звіт викладачеві і дайте відповідь на контрольні питання.

2.5 Зміст звіту

Звіт складається в електронному форматі і роздруковується. Звіт повинен містити:

- назву роботи;
- мету роботи;
- загальний вигляд інтерфейсу (головного вікна Wireshark);
- скріншот налаштувань мережевого адаптеру у програмі Wireshark;
- скріншоти з кадрами автентифікації (п.2.3), відповіді на поточні запитання.

2.6 Контрольні питання

1) Які основні стани проходить бездротовий клієнт перед тим, як почати передачу даних через точку доступу?
2) В чому полягає процес активного сканування бездротових мереж?
3) Які типи аутентифікації визначені в стандарті IEEE 802.11?
4) Як відбувається аутентифікація на основі попередньо встановлених ключів (PSK)?
5) Як перевести бездротовий адаптер в режим моніторингу в програмі Wireshark?
6) Який фільтр потрібно встановити в Wireshark для перегляду кадрів аутентифікації?
7) Скільки кадрів аутентифікації передається між клієнтом та точкою доступу в незахищеній мережі?
8) Які додаткові кадри, окрім аутентифікації, передаються в процесі асоціації клієнта з точкою доступу у захищеній мережі?

ДОДАТОК В

Удосконалення методики вивчення технології Wi-Fi

Жуковицький І.В., Компанієць В. В., Олійник К. О.,
Український державний університет науки і технологій, Україна

Wi-Fi (скорочено від «Wireless Fidelity») є технологією, що дозволяє електронним пристроям підключатися до мережі через радіохвилі без використання дротових з'єднань. Це особливо корисно для мобільних пристроїв, таких як смартфони, планшети та ноутбуки, але також використовується у стаціонарних комп'ютерах, телевізорах, принтерах та інших пристроях. На сьогодні це одна з найбільш популярних та затребуваних технологій. Тому удосконалення методики вивчення та застосування технології Wi-Fi, зокрема розгортання мереж Wi-Fi в інфраструктурному режимі та забезпечення їх безпеки є актуальним завданням.

Запропоновано покращену методику вивчення технології WiFi, яка акцентує увагу на практичних лабораторних роботах та аспектах безпеки. Наприклад, студенти можуть проводити експерименти з реальним обладнанням, налаштовувати параметри захисту, вивчати типові атаки та їх уникнення. Лабораторні роботи можуть включати в себе симуляцію атак для надання студентам можливості вивчати реальні сценарії безпеки Wi-Fi в контрольованому середовищі.

Для підготовки до проведення лабораторних робіт по розгортанню та захисту мережі Wi-Fi проведено успішне розгортання мережі WiFi в інфраструктурному режимі в кафедральній лабораторії з особливим акцентом на питання безпеки. Виділено важливі кроки налаштування точок доступу, роботу зі стандартами та використання додаткових засобів безпеки, зокрема аутентифікації та шифрування.

В процесі виконання лабораторних робіт розглядаються сучасні протоколи шифрування WPA2 та WPA3, а також їхня реалізація на точках доступу. Обговорюється важливість налагодження параметрів безпеки для запобігання несанкціонованому доступу та перехопленню інформації.

Одним із ключових аспектів безпеки є ефективна аутентифікація користувачів та шифрування передачі даних. В процесі виконання лабораторних робіт предбачається аналіз різних методів аутентифікації, включаючи використання паролів, сертифікатів та двофакторної аутентифікації. Розглядаються принципи роботи протоколів шифрування та їхня реалізацію на практиці.

Використання спеціалізованого програмного забезпечення є необхідною складовою навчального процесу. Програми, такі як Wireshark та Aircrack-ng, дозволяють студентам вивчати та аналізувати трафік мережі, виявляти потенційні загрози, вразливості мережі та ефективно застосовувати принципи захисту.

Впровадження покращеної методики вивчення технології WiFi та розгортання мереж в інфраструктурному режимі дозволить забезпечити високий рівень освоєння студентами технології мереж Wi-Fi. Крім того, аналіз та дослідження роботи мережі Wi-Fi, в процесі підготовки механізмів вивчення студентами цієї мережі на кафедрі ЕОМ, дозволить покращити якість та безпеку роботи цієї мережі.

ДОДАТОК Г

РОЗРОБКА КОМПЛЕКСУ ЛАБОРАТОРНИХ РОБІТ ПО ДОСЛІДЖЕННЮ МЕХАНІЗМІВ ЗАХИСТУ МЕРЕЖІ WI-FI

Компанієць В.В., керівник проф. Жуковицький І.В.
Український державний університет науки і технологій

З розвитком сучасних технологій мережі Wi-Fi стали необхідністю, що забезпечує зв'язок та доступ до інформації в сучасному світі. Ці бездротові мережі стали невід'ємною частиною нашого повсякденного життя, дозволяючи нам підключати пристрої та обмінюватися даними зі зручністю та мобільністю, яку важко переоцінити. Проте, разом із зростанням популярності та важливості мереж Wi-Fi, збільшилася і загроза їхній безпеці. Нестача належного захисту може призвести до небажаного доступу, витоку конфіденційної інформації та серйозних кібератак. Тому розробка комплексу лабораторних робіт для дослідження механізмів захисту мереж Wi-Fi є актуальною та важливою задачею в сучасному цифровому світі. Актуальність нашої роботи підкреслюється зростаючими обсягами даних, які передаються через бездротові мережі, і залежністю суспільства від безпеки цих мереж. З кожним новим підключеним пристроєм та розширенням покриття Wi-Fi, ризики стають ще більшими. Кіберзлочинці розвивають все більш схитрі та складні методи атак, і тільки ретельна підготовка та вивчення механізмів захисту може забезпечити ефективний контроль над безпекою мереж Wi-Fi. Зараз вже немає сумніву, що забезпечення безпеки мереж Wi-Fi є завданням першочергового значення, і ця тема заслуговує на нашу увагу і розвідку. Метою є розробка комплексу лабораторних робіт, спрямованих на вивчення та аналіз механізмів захисту мереж Wi-Fi. Ми прагнемо створити набір практичних завдань, які дозволять студентам і фахівцям у сфері інформаційної безпеки краще розуміти сутність проблем безпеки мереж Wi-Fi і виявляти їх вразливості. Дослідження буде спрямоване на розвиток практичних навичок і компетентностей, необхідних для забезпечення безпеки в бездротових мережах.

Перш за все було вирішено, що необхідно ознайомити студентів з протоколом 802.11i, в якому визначено використання аутентифікації на основі попередньо встановлених ключів (PSK) та аутентифікації на основі стандарту IEEE 802.1X. Далі з механізмами забезпечення конфіденційності та цілісності даних, для чого використовуються протоколи TKIP та CCMP. Також з набором функцій для забезпечення безпеки бездротових мереж, які визначені у програмі сертифікації WPA/WPA2. У WPA для забезпечення конфіденційності даних використовується протокол TKIP, у WPA2 – протокол CCMP.