МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Циклова комісія *комп'ютерних систем та мереж*
(повна назва циклової комісії)

Допустити до захисту
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
_____ *Ірина КРАВЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)
« *10* » *06* 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
ФАХОВИЙ МОЛОДШИЙ БАКАЛАВР

Тема: *Дослідження інтеграції засобів шифрування даних та методів авторизації користувачів*

Група: *3-013* Спеціальність: *123 «Комп'ютерна інженерія»*

Здобувач освіти _____ *Данило БАЛАЦЬКИЙ*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Галина ДАНИЛІНА*
(підпис) (ім'я, ПРІЗВИЩЕ)

Консультант з оформлення пояснювальної записки _____ *Оксана ОСАДЧА*
(підпис) (ім'я, ПРІЗВИЩЕ)

Кривий Ріг 2025 р.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Відділення *комп'ютерної та програмної інженерії*
Циклова комісія *комп'ютерних систем та мереж*
Освітній ступінь *фаховий молодший бакалавр*
Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК* (ім'я, ПРІЗВИЩЕ)
« *01* » *03* 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ОСВІТИ

Балацькому Данилу Андрійовичу
(прізвище, ім'я, по батькові)

1.Тема роботи *Дослідження інтеграції засобів шифрування даних та методів авторизації користувачів*

Керівник роботи *Даниліна Галина Володимирівна – викладач, «спеціаліст вищої категорії», КТН, доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по коледжу від « *04* » *04* 2025 року № *50-ст*

2. Строк подання здобувачем освіти роботи з *01.03.2025* по *15.06.2025*

3. Вихідні дані до роботи *Устаткування для побудови системи захисту мережі WI-FI.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) *Аналіз технології побудови бездротових комп'ютерних мереж. Безпека мереж Wi-Fi. Проектування захищеної мережі Wi-Fi.*

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

6. Консультанти розділів роботи (проекту)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	*Узгодження технічного завдання*	*01.03.2025*	
2	*Огляд літератури по темі*	*15.03.2025*	
	кваліфікаційної роботи		
3	*Аналіз технології побудови бездротових*	*28.04.2025*	
	комп'ютерних мереж		
4	*Безпека мереж Wi-Fi*	*14.05.2025*	
5	*Проектування захищеної мережі Wi-Fi*	*26.05.2025*	
6	*Оформлення пояснювальної записки*	*06.06.2025*	
7	*Захист кваліфікаційної роботи*		

Здобувач освіти _____ *Данило БАЛАЦЬКИЙ*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Галина ДАНИЛІНА*
(підпис) (ім'я, ПРІЗВИЩЕ)

StrikePlagiarism.com

Дата звіту 5/26/2025

Дата редагування ---

Документ прийнятий

Звіт подібності

метадані

Назва організації

Ukrainian national aviation university

Заголовок

Балацький Д_3-013_2025_КПІ

Автор Науковий керівник / Експерт

Балацький ДГринченко О

підрозділ

Криворізький Фаховий коледж

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

10.53%
10.53%
КП 1

1.10%
1.10%
КЦ

25
Довжина фрази для коефіцієнта подібності 2

10512
Кількість слів

79384
Кількість символів

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Дослідження інтеграції засобів шифрування даних та методів авторизації користувачів» викладена на 63 с., містить 18 рис., 1 табл. 18 використаних літературних джерел.

WI-FI МЕРЕЖА, ШИФРУВАННЯ, АВТОРИЗАЦІЯ, RADIUS-СЕРВЕР, MAC-АДРЕСА, VPN

Поєднання сучасних алгоритмів шифрування даних та авторизації користувачів за допомогою *RADIUS*-сервера дає максимальний захист мережі. Легке додавання користувачів дає можливість налаштувати гнучку мережеву структуру. Захищена мережа дасть змогу зберегти конфіденційність, цілісність та автентичність інформації та уникнути збитків від зламу мережі.

Метою роботи є проектування та налаштування системи захисту мережі *Wi-Fi*, що дозволить запобігти несанкціонованому доступу до мережі та крадіжці корпоративної інформації.

Результати кваліфікаційної роботи можуть бути використані при проектуванні системи захисту мережі *Wi-Fi* в невеликому офісі чи вдома.

Прогнозові припущення щодо розвитку об’єкту дослідження — використання ефективних методів в системі безпеки мережі дає можливість забезпечити стабільну роботу мережі, уникнути інформаційних та фінансових втрат. Із стрімким розвитком бездротових технологій пошук нових методів і підходів є дуже актуальною темою.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ТЕРМІНІВ

LAN (*Local Area Networks*) – локальна обчислювальна мережа

Wi-Fi (*Wireless Fidelity* — «бездротова точність») – бездротова мережа, стандарт на обладнання *Wireless LAN*.

CSMA/CD (*Carrier Sense Multiply Access with Collision Detection*) – метод колективного доступу з впізнаванням несучої і виявленням колізії.

IEEE (*Institute of Electrical and Electronics Engineers*) – міжнародна, некомерційна, асоціація фахівців в галузі техніки, світовий лідер в області розробки стандартів по радіоелектроніці та електротехніці.

MAC (Media Access Control) – рівень управління доступом до носія.

LLC (Logical Link Control) – рівень управління логічним каналом.

ВОК – волоконно-оптичний кабель.

Стек протоколів *TCP/IP* (*Transmission Control Protocol/Internet Protocol*) - набір мережевих протоколів різних рівнів моделі мережевої взаємодії *DOD*, що використовуються в мережах.

IP-адреса (*Internet Protocol Address*) - мережева адреса вузла в комп'ютерній мережі, побудована за протоколом *IP*. При зв'язку через мережу інтернет потрібно глобальна унікальність адреси, у випадку роботи в локальній мережі потрібно унікальність адреси в межах мережі.

DNS (*Domain Name System* — система доменних імен) — комп’ютерна розподілена система для отримання інформації про домени.

DHCP (англ. *Dynamic Host Configuration Protocol* - протокол динамічної конфігурації вузла) - це мережевий протокол, що дозволяє комп'ютерам автоматично отримувати *IP*-адресу та інші параметри, необхідні для роботи в мережі *TCP/IP*. Даний протокол працює за моделлю «клієнт-сервер».

ПК – персональний комп’ютер.

ЛЗ – лінії зв’язку.

ВСТУП

Сьогодні бездротові технології стали критично важливими, особливо для бізнесу. Мобільність та миттєвий доступ до інформації дозволяють командам працювати значно продуктивніше, швидше та ефективніше, порівняно з часами дротових з'єднань.

Питання безпеки бездротових мереж завжди було актуальним, особливо для великих корпоративних мереж. Для спокійного користування мережею необхідно забезпечити три ключові аспекти:

- **Конфіденційність:** Дані повинні бути надійно зашифровані, щоб їх не могли перехопити сторонні.
- **Цілісність:** Важливо гарантувати, що дані не будуть непомітно змінені під час передачі.
- **Автентичність:** Необхідно мати впевненість, що дані надходять від легітимного джерела.

Метою кваліфікаційної роботи є проектування та налаштування ефективної системи захисту *Wi-Fi* мережі, яка запобігатиме несанкціонованому доступу та витоку цінної інформації.

Для досягнення цієї мети ми плануємо:

1. Проаналізувати сучасні засоби та методи забезпечення безпеки бездротових мереж.

2. Спроектувати оптимальну систему захисту для конкретної мережі.

3. Розробити алгоритми функціонування та програмний код для налаштування цієї системи захисту.

Об'єктом нашого дослідження є система безпеки *Wi-Fi* мережі, з акцентом на комбінації методів шифрування даних та авторизації користувачів.

РОЗДІЛ 1
АНАЛІЗ ТЕХНОЛОГІЇ ПОБУДОВИ БЕЗДРОТОВИХ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Стандарти бездротових комп'ютерних мереж

Сьогодні складно уявити повсякдення без *Bluetooth*-з'єднань чи можливості миттєво "серфити" інтернет, сидячи будь-де – навіть на сходах університету. Те, що колись здавалося магією, стало звичною рутиною. Ще зовсім недавно бездротові технології використовувалися переважно у сфері торгівлі. Проте, з кінця 90-х років минулого століття локальні бездротові мережі (*WLAN*), відомі нам як *Wi-Fi*, почали стрімко розвиватися. Ці технології подарували нам свободу переміщення та можливість залишатися в курсі подій незалежно від нашого місцезнаходження, ставши по суті мобільною еволюцією дротових мереж.

Окрім основних стандартів *Wi-Fi* (802.11*a*/*b*/*g*/*n*/*ac*/*ax*/*be*), існує низка допоміжних стандартів, які розширюють функціональність та адаптують технологію до різних потреб і умов:

- 802.11*c* (неактивний): Цей стандарт був спрямований на стандартизацію параметрів бездротових мостів (точок доступу) для забезпечення сумісності між обладнанням різних виробників. На сьогодні його функціональність інтегрована в основні стандарти.
- 802.11*d* (регуляторні норми): Цей стандарт визначає фізичні параметри радіоканалів (потужність передавача, діапазони частот) та бездротових пристроїв для відповідності законодавчим вимогам різних країн. Він гарантує, що *Wi-Fi* обладнання працює в рамках дозволеного спектру та з безпечною потужністю в кожному регіоні.

Таблиця 1.1 - Характеристики основних стандартів бездротових мереж

Стандарт	Частотний діапазон	Максимальна швидкість передачі даних (теоретична)	Типовий радіус дії (у приміщенні)	Кількість непересічних каналів (залежно від ширини каналу та регіону)	Основні особливості
802.11*b*	2.4 ГГц	11 Мбіт/сек	30-50 м	3	Застарілий, низька швидкість, чутливий до перешкод.
802.11*g*	2.4 ГГц	54 Мбіт/сек	30-75 м	3	Застарілий, краща швидкість, ніж 802.11*b*, але все ще чутливий до перешкод.
802.11*a*	5 ГГц	54 Мбіт/сек	20-35 м	8-25 (залежно від ширини каналу)	Застарілий, менше перешкод, ніж у 2.4 ГГц, але менший радіус дії.
802.11*n* (*Wi-Fi* 4)	2.4/5 ГГц	До 600 Мбіт/сек (з *MIMO*)	25-75 м	3 (у 2.4 ГГц), більше у 5 ГГц (залежно від ширини каналу)	Підтримка *MIMO* (кілька антен для одночасної передачі), значно вища швидкість.
802.11*ac* (*Wi-Fi* 5)	5 ГГц	До кількох Гбіт/сек (з *MU-MIMO*)	20-60 м	Багато (залежно від ширини каналу, до 80 або 160 МГц)	Підтримка *MU-MIMO* (одночасне обслуговування кількох клієнтів), дуже висока швидкість.
802.11*ax* (*Wi-Fi* 6)	2.4/5/6 ГГц	До 9.6 Гбіт/сек (з *MU-MIMO* та *OFDMA*)	Залежить від діапазону та умов	Більше, ніж у попередніх стандартах (завдяки *OFDMA*)	Підвищена ефективність, краща робота у завантажених мережах, підтримка 6 ГГц.
802.11*be* (*Wi-Fi* 7)	2.4/5/6 ГГц	До 46 Гбіт/сек (з *MU-MIMO*, *OFDMA* та *MLO*)	Залежить від діапазону та умов	Ще більше (завдяки ширшим каналам та *OFDMA*)	Очікується значне збільшення швидкості, зменшення затримки, підтримка *MLO*.

- 802.11*e* (*QoS* для мультимедіа): Цей стандарт впроваджує механізми пріоритезації трафіку, оптимізовані для передачі аудіо- та відеопотоків. Це дозволяє

забезпечити більш стабільну та якісну роботу мультимедійних додатків, зменшуючи затримки та переривання під час потокового відтворення.

- 802.11*f* (*IAPP - Inter-Access Point Protocol*, застарілий): Цей стандарт визначав протокол для взаємодії між точками доступу під час роумінгу клієнта між різними сегментами мережі. Він мав забезпечити безшовний перехід між точками доступу без втрати з'єднання. На сьогодні його функціональність значною мірою замінена вдосконаленими механізмами роумінгу в наступних стандартах, зокрема 802.11*r*.
- 802.11*h* (динамічне керування спектром): Цей стандарт був розроблений для вирішення проблем використання діапазону 5 ГГц у Європі, де він частково використовувався супутниковим зв'язком. 802.11*h* впровадив механізми динамічного регулювання потужності передавача та вибору частоти для запобігання перешкодам іншим системам.
- 802.11*i* (підвищена безпека): Цей стандарт значно підвищив рівень безпеки бездротових мереж, запровадивши надійніші протоколи шифрування та аутентифікації. Ключовим елементом став протокол *AES* (*Advanced Encryption Standard*) з підтримкою ключів різної довжини (128, 192, 256 біт), що забезпечило високий рівень захисту даних. Сумісність з 802.11*i* стала важливою характеристикою для сучасних бездротових пристроїв.
- 802.11*j* (спеціально для Японії): Цей стандарт був розроблений спеціально для Японії та розширював можливості стандарту 802.11*a*, додаючи додатковий діапазон частот у 4.9 ГГц.
- 802.11*n* (*Wi-Fi* 4, застаріває): Хоча в оригінальному тексті він згадується як перспективний, 802.11*n* (*Wi-Fi* 4) вже є поширеним, але поступово застаріває стандартом. Він значно збільшив пропускну здатність мереж (до 600 Мбіт/с) завдяки використанню технології *MIMO* (*Multiple-Input Multiple-Output*), що передбачає використання кількох антен для одночасної передачі та прийому даних.

- 802.11*r* (*Fast Transition* - швидкий перехід): Цей стандарт визначає механізми швидкого та безшовного роумінгу між точками доступу в одній мережі. Він мінімізує час перепідключення при переміщенні користувача між зонами покриття різних точок доступу, забезпечуючи безперервність з'єднання для таких застосунків, як *VoIP* та потокове відео.
- 802.11*s* (*Mesh*-мережі): Цей стандарт описує архітектуру та протоколи для побудови самоорганізованих *Mesh*-мереж. У таких мережах кожен вузол (точка доступу) може не лише передавати дані клієнтам, але й ретранслювати трафік від інших вузлів. Це значно збільшує зону покриття, підвищує надійність мережі (завдяки резервним шляхам передачі даних) та може збільшити загальну пропускну здатність. *Mesh*-мережі динамічно визначають оптимальні маршрути передачі та самовідновлюються у випадку виходу з ладу окремих вузлів. Сучасні *Mesh Wi-Fi* системи для дому та офісу є практичною реалізацією цього стандарту.

Ці допоміжні стандарти демонструють постійний розвиток технології *Wi-Fi*, спрямований на покращення продуктивності, безпеки, надійності та адаптації до різноманітних сценаріїв використання.

1.2 Топології бездротових комп’ютерних мереж

Будь-яка бездротова мережа зазвичай складається як мінімум з однієї точки доступу (роутера) та одного або кількох клієнтів (смартфонів, ноутбуків тощо), що знаходяться в зоні її покриття. Кількість та конфігурація цих елементів визначають різні топології бездротових мереж:

- Незалежні базові набори послуг (*Independent Basic Service Sets, IBSSs*): Це однорангові (*peer-to-peer*) мережі, де клієнти (пристрої з *Wi-Fi*) з'єднуються безпосередньо один з одним без використання центральної точки доступу. Таку топологію також називають *ad-hoc* мережею або мережею "точка-точка". Уявіть собі

ситуацію, коли кілька ноутбуків обмінюються файлами напряму, без підключення до *Wi-Fi* роутера. Раніше такі з'єднання часто використовували стандарт 802.11*b* з обмеженою швидкістю, але сьогодні сучасні пристрої можуть створювати *ad-hoc* мережі з використанням новіших та швидших стандартів *Wi-Fi*.

- Базові набори послуг (*Basic Service Sets, BSSs*): Це найбільш поширений тип бездротової мережі, що включає одну центральну точку доступу (*Access Point, AP*), яка служить посередником для зв'язку між усіма клієнтами в її зоні покриття. Усі пристрої в мережі *BSS* комунікують через цю точку доступу. Домашні *Wi-Fi* мережі та більшість офісних мереж побудовані за цією топологією. Точка доступу постійно транслює ідентифікатор набору послуг (*Service Set Identifier, SSID*), тобто ім'я мережі, щоб клієнтські пристрої могли її ідентифікувати та підключитися.

- Розширені набори послуг (*Extended Service Sets, ESSs*): Ця топологія використовується для створення більших бездротових мереж, що охоплюють значні території (наприклад, великі офісні будівлі, кампуси). *ESS* складається з кількох базових наборів послуг (*BSSs*) з кількома точками доступу, які об'єднані через дротову мережу (зазвичай *Ethernet*). Усі ці точки доступу мають однаковий *SSID*, створюючи єдину логічну бездротову мережу. Це дозволяє користувачам плавно переміщатися між зонами покриття різних точок доступу (роумінг) без втрати з'єднання. Сучасні системи *Mesh Wi-Fi* також є прикладом розширених наборів послуг, де точки доступу можуть взаємодіяти без прямого дротового з'єднання, але при цьому забезпечують єдину безшовну мережу.

Отже, зона обслуговування – це фактично область покриття бездротової мережі, утворена однією або кількома точками доступу, що об'єднують мережеві пристрої. Трансляція *SSID* є ключовим механізмом, що дозволяє клієнтам знаходити та приєднуватися до потрібної бездротової мережі.

Рисунок 1.1 - З'єднання *Ad-Hoc*

Ad-hoc мережі (*IBSS*): Мережа без посередників

У цьому типі бездротової мережі клієнтські пристрої (ноутбуки, смартфони тощо) самостійно об'єднуються в мережу для спільного використання ресурсів без необхідності центральної точки доступу (роутера). Зазвичай такі мережі є невеликими за розміром та створюються ситуативно в межах певної території. Вони часто не мають підключення до провідної мережі та теоретично не мають обмежень на кількість підключених пристроїв.

Однією з проблем в *ad-hoc* мережах є так звана проблема "прихованого вузла", оскільки всі пристрої мають рівні права на передачу даних. Щоб уникнути колізій, коли кілька пристроїв починають передавати одночасно, в мережі використовується механізм маячкового інтервалу (*beacon interval*). Пристрій, що ініціює передачу, періодично надсилає маячковий сигнал, який містить таймер синхронізації (*Timer Synchronization Function, TSF*). Всі учасники мережі синхронізують свої таймери за найшвидшим з них, забезпечуючи таким чином координацію передачі даних в межах однієї незалежної базової зони обслуговування (*IBSS*).

Інфраструктурні мережі (*BSS*): Зв'язок через точку доступу

На відміну від *ad-hoc* мереж, базова зона обслуговування (*BSS*) використовує центральний елемент – точку доступу (*Access Point, AP*) або, простіше кажучи, *Wi-Fi* роутер. Усі клієнтські пристрої в мережі *BSS* зв'язуються між собою виключно через цю точку доступу. Коли один клієнт хоче передати інформацію іншому, він спочатку надсилає її точці доступу, а вже вона перенаправляє дані до отримувача.

Точка доступу зазвичай має *uplink*-порт (часто *Ethernet*), який використовується для підключення *BSS* до провідної мережі, наприклад, до локальної мережі або інтернету. Така модель є найбільш поширеною для з'єднання більшої кількості комп'ютерів в офісах, будинках та громадських місцях. Сучасні точки доступу часто виконують функції роутера, самостійно розподіляючи інтернет-канал між підключеними пристроями та забезпечуючи базовий рівень мережевої безпеки.

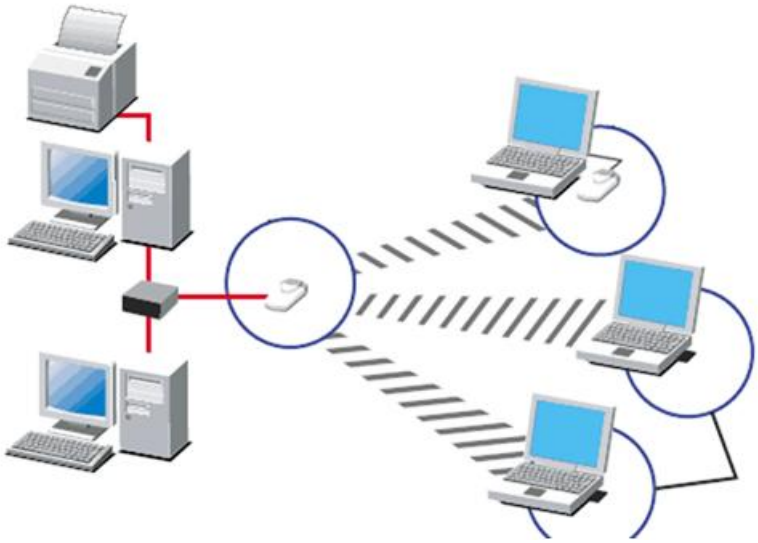

Рисунок 1.2 - Мережа *BSS*

Точка доступу (*Access Point*) з підключенням до інтернету:

У цьому найпоширенішому сценарії точка доступу (яка часто інтегрована в *Wi-Fi* роутер) підключається до модема (який також може бути об'єднаний з роутером в одному пристрої). Роутер виконує функцію маршрутизації трафіку між локальною бездротовою мережею та інтернетом. Будь-який комп'ютер або інший пристрій з *Wi-Fi* адаптером, що знаходиться в зоні покриття цієї точки доступу, отримує доступ до інтернету. Це стандартна схема для домашніх та малих офісних мереж.

Режим клієнтської точки доступу (*Client Mode*):

У цьому режимі бездротовий пристрій (зазвичай точка доступу або *Wi-Fi* адаптер) працює як клієнт іншої інфраструктурної мережі (*BSS*). Він підключається до існуючої точки доступу, подібно до ноутбука або смартфона. Однак, у класичному

варіанті цього режиму, до такого "клієнта" можна підключити лише один пристрій з певною *MAC*-адресою. Цей режим часто використовувався для бездротового підключення пристроїв, які спочатку не мали вбудованого *Wi-Fi*, наприклад, стаціонарних комп'ютерів або принтерів, до існуючої бездротової мережі. Сучасні ж пристрої часто підтримують режим *Wi-Fi Bridge* або *Repeater*, який дозволяє не лише підключатися до існуючої мережі, але й розширювати її, підключаючи кілька клієнтів.

Декілька базових зон обслуговування (*BSSs*), об'єднаних через дротову розподільчу систему (*Distribution System, DS*), утворюють розширену зону обслуговування (*Extended Service Set, ESS*), забезпечуючи безшовний роумінг для користувачів на більшій території.

Мостове з'єднання (*Bridging*):

У цьому режимі бездротові точки доступу використовуються для з'єднання двох або більше окремих дротових мереж через бездротовий канал зв'язку. Уявіть собі два офіси в сусідніх будівлях, кожен зі своєю локальною дротовою мережею. За допомогою двох точок доступу, налаштованих у режим моста, ці мережі можна об'єднати без прокладання кабелю між будівлями. Важливо зазначити, що в режимі моста точка доступу зазвичай не призначена для безпосереднього підключення бездротових клієнтів. Її основна функція – прозоре з'єднання двох або більше дротових сегментів мережі на канальному рівні.

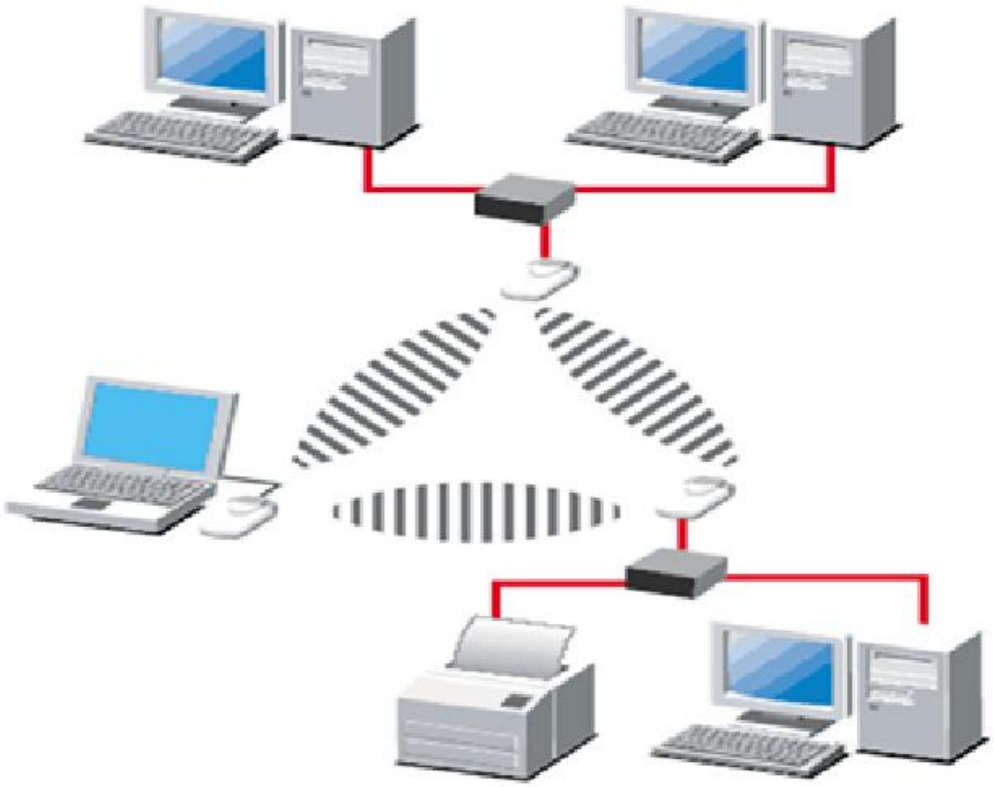

Рисунок 1.3 - Мостове з’єднання

1.3 Засоби побудови бездротових комп’ютерних мереж

Діапазон 2,4 ГГц перевантажений різними системами - бездротові телефони, пристрої *Bluetooth*.

У США для безліцензійної роботи мереж стандарту *IEEE* 802.11*a* в діапазоні 5,1-5,9 ГГц виділені смуги 5,15-5,35 і 5,725-5,825 ГГц. Всього 300 МГц у порівнянні з 83 МГц у діапазоні 2,4 ГГц. Замість трьох каналів, що не перекриваються, у діапазоні 2,4 ГГц для мереж *IEEE* 802.11*b* тільки в нижньому під діапазоні 5,15-5,35 ГГц маються вісім каналів, що не перекриваються. Аналогічна ситуація в Європі і Україні - у більш високочастотній області ширина смуги частот ще більше.

Виробники розробили дводіапазонні чипсети для забезпечення сумісності абонентського устаткування з мережами стандартів IEEE 802.11*a*/*b*.

Пристрої *IEEE* 802.11*g* з 2002 року роблять такі компанії, як *Buffalo Technologies, Linksys, D-Link, Apple*. Пізніше до них приєдналися фірми *Netgear, Belkin, Actiontec, Proxim* і багато інших. Таку можливість їм надали виробники наборів мікросхем для 802.11*g* (насамперед компанії *Intersil, Atheros Communications, Broadcom*).

На території України використання *Wi-Fi* регулюється УДЦР (Український державний центр радіочастот). Без спеціального дозволу можна користуватися мережею з точкою доступу зі стандартною все направленою (4-10 Дб, потужність сигналу до 500мВт на 2.4ГГц и 200мВт на 5ГГц) для внутрішніх потреб організації (Рішення Національної комісії по регулюванню зв'язку на Україні № 914 от 2007.09.06) . Якщо виникає потреба у потужнішому сигналі або необхідність доступу в Інтернет, необхідно зареєструвати передавач та отримати ліцензію в УДЦР.

В основу мереж *Wi-Fi* покладено принцип обміну інформацією без використання дротів. Данні або інформація в мережі можуть бути представлені у вигляді електронної пошти, *Web*-сторінок, відео, музики, речового повідомлення.

Для передачі всі данні перетворюються в символьну форму за допомогою електричних, світлових, радіосигналів. В основі сигналу лежить передача електромагнітних хвиль довжиною від міліметра через повітряний простір від однієї точки мережі до іншої.

В залежності від місця мережі сигнали можуть бути цифровими та аналоговими. Для передачі мережа перетворює цифровий сигнал на аналоговий.

Цифровий сигнал (*digital signal*) може різко змінювати свою амплітуду (див. рис. 1.4). Зазвичай він бінарний та має 2 стани: 0 та 1 і розглядається як послідовний набір біт. Ця форма сигналу найкраще підходить для обробки та зберігання на цифрових пристроях.

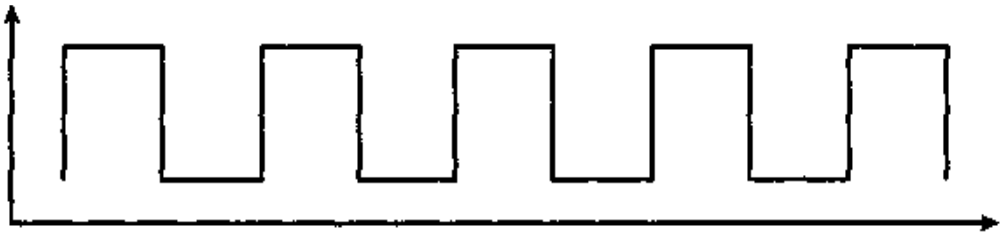

Рисунок 1.4 - Цифровий сигнал

Цифрові сигнали легко регенеруються, тому їх можна передавати на великі відстані, періодично відтворюючи і очищуючи від перешкод та шуму. Для забезпечення захисту такі сигналі достатньо легко шифрувати та дешифрувати – переставити біти місцями згідно певного методу шифрування.

Цифрову передачу даних можна охарактеризувати двома показниками:

- швидкість передачі даних – це швидкість, з якою цифрові сигнали передають дані по мережі. Ця величина є показником загальної кількості біт, що були передані за час їх передачі. Одиницею виміру є кількість біт за секунду.

- пропускна здатність – це швидкість , з якою по мережі проходить лише корисна інформація, тобто інформаційний потік без службових фреймів (полів контролю помилок, фреймів підтвердження , сигналів заголовків або часу потраченого на повторну передачу у разі помилки). Цей показник демонструє продуктивність та ефективність роботи мережі.

Але має суттєвий недолік: при зростанні кількості користувачів мережі підвищується рівень конкуренції для отримання доступу до середовища, всі пристрої знаходяться в режимі очікування і це призводить до значного зниження пропускної здатності.

Аналогові сигнали (*analog signal*) (див. рис. 1.5) – це сигнал, якому властива зміна амплітуди з часом.

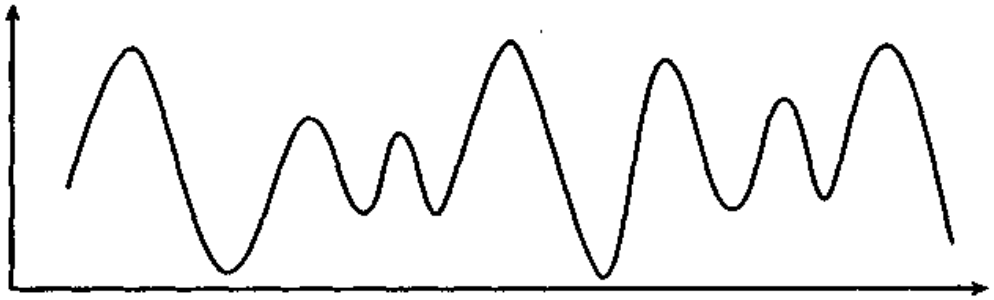

Рисунок 1.5 - Аналоговий сигнал

В бездротових мережах сигнали знаходяться в діапазоні 2,4 ГГц та належать до діапазону радіохвиль. Радіохвилі (*RF-signals*) – це електромагнітні хвилі, що передаються від антени передавача до антени приймача. Аналогові сигнали характеризуються такими параметрами, як (див. рис. 1.6) :

- амплітуда – визначає інтенсивність радіосигналу. Мірою амплітуди є потужність. Чим більша потужність сигналу тим більша відстань , на яку він передається.

- частота (*frequency*) – це показник, що характеризує скільки разів за секунду сигнал повторює себе, тобто кількість циклів, що відбуваються за секунду.

- фаза (*phase*) – параметр, що демонструє наскільки сигнал відхилився від початкового положення (початкової точки поширення). Зміна фази застосовується для передачі інформації. Через уникнення впливу затухання сигналу при розповсюдженні на велику відстань цей спосіб є дуже ефективним.

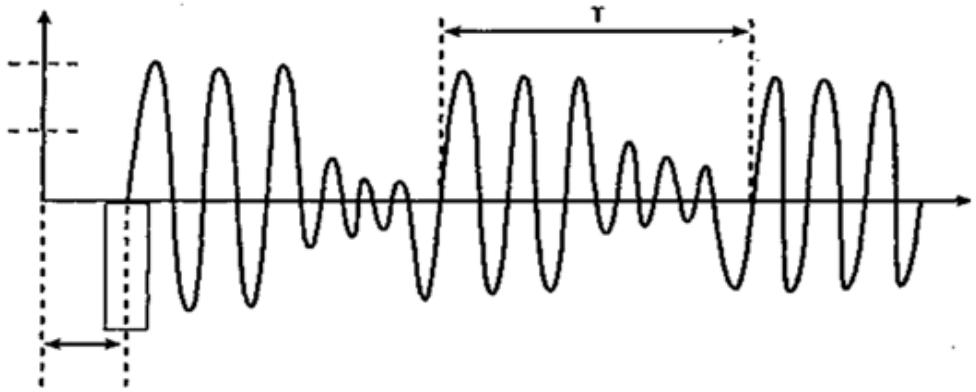

Рисунок 1.6 - Параметри аналогових сигналів

Серед переваг використання радіохвиль слід зауважити, що вони можуть передавати інформацію на достатньо великі відстані при відсутності прямих перешкод. Не впливають на показники природні явища (туман). Використання частот не потребує ліцензування у більшості випадків.

Але присутні і негативні сторони. Це невелика пропускна здатність, істотно мала перешкодостійкість від інших хвиль та шумів, а також незахищеність, оскільки хвилі можуть розповсюджуватися за межі приміщень та піддавати ризику інформацію.

Щоб передати дані по мережі необхідно цифрові сигнали, що зберігаються в комп'ютері, перетворити на радіосигнали. Цю функцію виконує модем (модулятор/демодулятор). Він не тільки перетворює цифровий сигнал в аналоговий , а ще виконує накладання інформаційної складової на основну несучу (*carrier signal*, електромагнітна хвиля певної частоти). Накладання відбувається шляхом зміни параметрів несучої частоти за допомогою моделюючого сигналу. Можна змінювати амплітуду, фазу, частоту. У ролі несучої частоти виступає синусоїда (див. рис. 1.7).

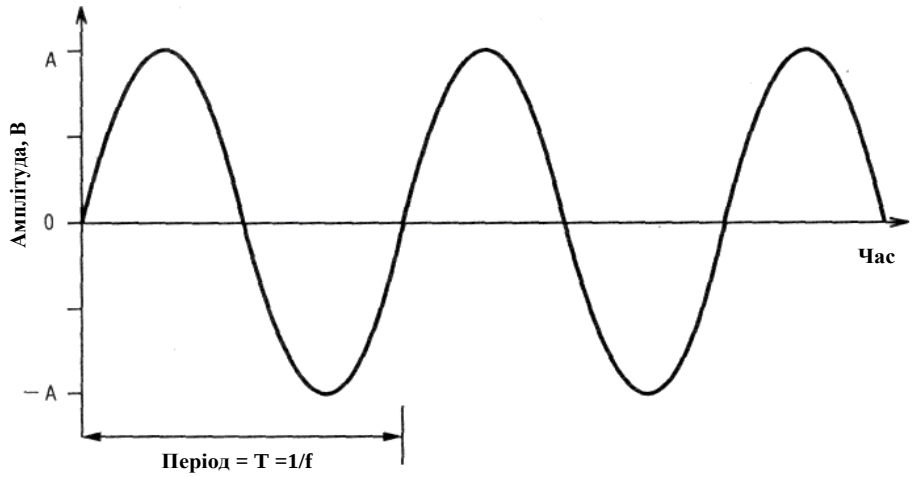

Рисунок 1.7 - Несуча частота

Модулятор передавача змішує інформаційний сигнал з несучим сигналом. Передавач передає підсилений сигнал на антену і сигнал розповсюджується по

середовищу. Антена отримувача приймає сигнал та демодулятор виділяє інформаційну складову.

Види модуляції:

- амплітудна (*Amplitude - Shift Keying, AASK*) модуляція (див. рис. 1.8.а). Логічні 1 та 0 відповідають різним рівням амплітудної синусоїди. Амплітудна модуляція слабко захищена від перешкод тому рідко застосовується. В основному у поєднанні з фазовою.

- частотна (*Frequency - Shift Keying, FSKK*) модуляція (див. рис. 1.8.б). Логічні 1 та 0 передаються синусоїдою з різною частотою. Не потребує складних схем реалізації, тому застосовується в низько швидкісних модемах.

- фазова (*Phase - Shift Keying, PSK*) модуляція 0 та 1 відповідають сигналам з різною фазою (див. рис. 1.8.в).

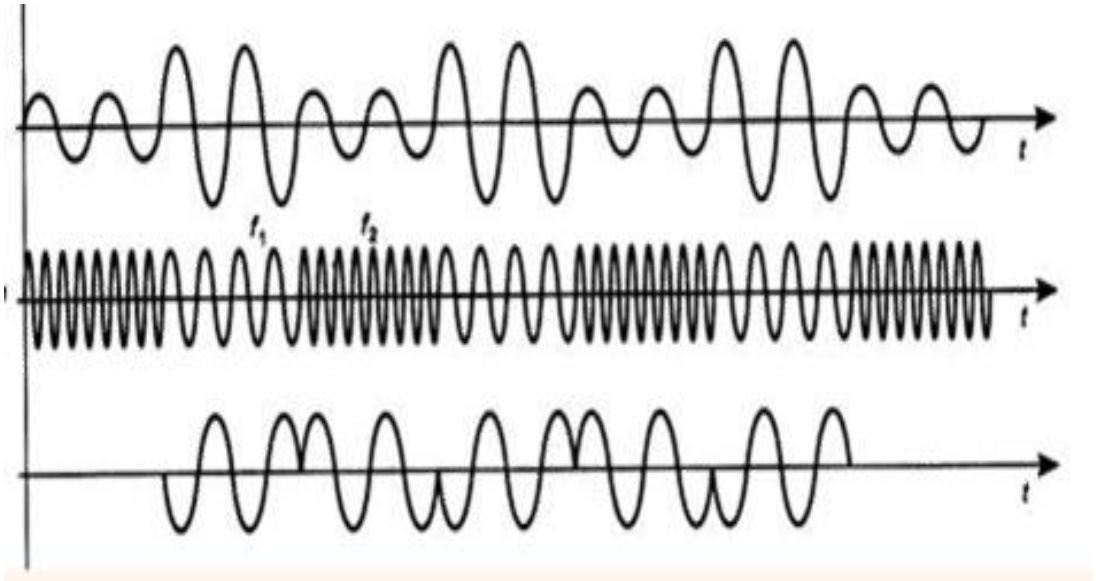

Рисунок 1.8 - Види модуляцій: а) амплітудна ; б) частотна;
в) фазова

Найчастіше використовують фазово-амплітудну модуляцію у швидкісних модемах. Так звана квадратурно-амплітудна модуляція (*quadrature amplitude modulation, QAM*). Передбачається зміна фази та амплітуди, що дає змогу передавати

в одній комбінації фази та амплітуди передавати велику групу символів. Використовується в мережах з високими швидкостями.

Не менш відома технологія розширення спектра (*spread spectrum*). Цей спосіб дозволяє значно знизити внутрішні і зовнішні перешкоди. Суттю методу є розподілення потужності сигналу в широкому діапазоні частот. Реалізують підхід за допомогою методу прямої послідовності (несуча модулюється цифровим кодом зі швидкістю передачі більшою ніж полоса частот інформаційного сигналу) або за технологією перестрибування з частоти на частоту (частота носія різко змінюється з одного значення на друге в заданому діапазоні).

Ще один метод - мультиплексування з розподіленням по ортогональних частотах (*orthogonal frequency division multiplexing, OFDM*) передбачає розподіл модулюючого сигналу по кільком підканалам, що належать одному каналу. Таким чином відбувається розпаралелювання сигналу і зростання швидкості його передачі.

Проходження інформаційного потоку через середовище провокує зміну його форми для досягнення оптимальних умов. Процес передачі інформації залежить від такої характеристики мережі як метод доступу.

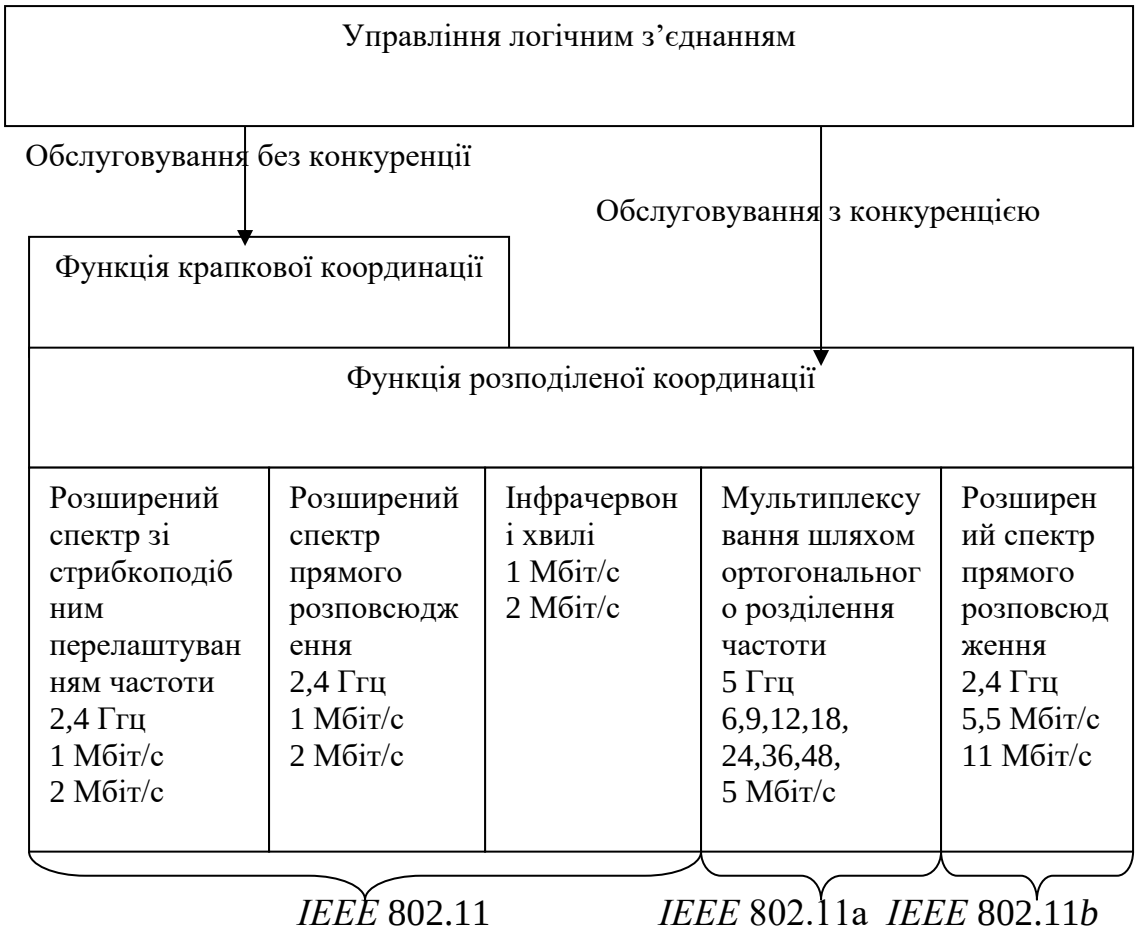

Рисунок 1.9 - Рівень *MAC*

РОЗДІЛ 2
БЕЗПЕКА МЕРЕЖ *WI-FI*

2.1 Інформаційна безпека в бездротових мережах

Безпека інформації в бездротових мережах є найбільш актуальною і важливою темою на сьогодні. Для порушників спосіб передачі інформації через радіоефір є найкращим, щоб перехопити, обробити та використати інформацію зі своєю метою. Радіоканал не забезпечує високого рівня захисту від прослуховування. Щоб проникнути в бездротову мережу не потрібно підключатися до дротів, досить опинитися в зоні прийому сигналу.

Мережа функціонує в діапазоні 2,4 ГГц, тому є вразливою для пристроїв, що працюють на тій самій частоті.

В наш час інформаційні потоки несуть в собі як приватні так і державно-важливі дані, порушення цілісності яких може призвести як до величезних збитків так і до катастроф. Впливи на мережу можна розмежувати на спеціально направлені дії порушників, помилки операторів та обслуговуючого персоналу, збої, відмови, аварії, які можуть призвести до розповсюдження інформації (порушення її конфіденційності), зміні (порушені цілісності), втраті, порушенню чи обмеженню доступу до неї.

Такі дії можуть спричинити цілий спектр проблем, пов'язаний з втратою матеріальних та інформаційних ресурсів.

Інформаційну безпеку можна визначити як захищеність інформаційних ресурсів власника, а також як захищеність мереж та їх компонентів від стороннього втручання від стороннього втручання. Стороннє втручання – це загроза або атака. Вона полягає в заподіянні певних дій, що базуються на захоплені, зміні, розповсюдженні інформації з метою завдання шкоди власнику.

При здійсненні атака порушує головні властивості інформації, а саме її доступність (забезпечувати своєчасне обслуговування мережевих запитів та доступ користувачів до потрібної їм інформації, тобто знайомство з інформацією, обробка, копіювання, зміна чи знищення); зберігання цілісності (тобто зберігати свій початковий вигляд, не зазнаючи будь - яких змін чи впливів). Спеціальні втручання з метою дезінформації, компрометації та зміни можуть не тільки завдати проблем, а й порушити функціонування мережі вцілому.

Конфіденційність (властивість інформації бути доступною тільки певній групі людей, що мають на це право, і бути таємною для користувачів, що не мають такого права). Під час атаки порушується право власника на інформацію, через що він може зазнати збитків.

Зі щоденним зростанням загроз досягти бездоганного рівня безпеки неможливо. Це пов’язано зі щоденним зростанням числа персональних комп’ютерів, стрімким розростанням локальних та регіональних мереж, коли процеси обміну інформацією охоплюють все більше сфер діяльності людини, і зростанням кола користувачів, що мають доступ до значних ресурсів та даних. Також відіграє вирішальну роль і відсталість рівня систем безпеки від технологій сьогодення.

Доступність на сьогодні засобів злому, хакерського програмного забезпечення дають змогу непрофесіоналам здійснювати атаки та завдавати шкоду установам та іншим користувачам а зростання кількості інформації в електронному вигляді, що зберігається та оброблюється в мережах, тільки поліпшує умови для нападів. Розвиток глобальної мережі як Інтернет лише сприяє здійсненню атак з будь-якої точки світу.

Значну роль відіграють недоліки в створеному програмному та апаратному забезпечені. Через шалені темпи розвитку виробники не допрацьовують деталі, якими потім користуються зламники або через які системи втрачають працездатність та відбувається втрата інформації.

Забезпечення безпеки комп’ютерних мереж полягає в організації дій спрямованих перешкодити будь-якому сторонньому втручанню в роботу мережі та

будь-яким спробам зміни, викрадення, порушення працездатності її компонентів, як інформаційних ресурсів так і програмних та апаратних засобів.

Серед основних засобів забезпечення безпеки інформації виділяють:

- правові
- морально-етичні
- організаційні
- технічні
- програмні

Законодавчі передбачають і регулюють створення, обробку, передачу інформації обмеженого доступу та визначають відповідальність за порушення цих норм.

До морально-етичних можна віднести людські якості або певні домовленості, що не дозволяють користувачу порушувати інформаційну безпеку або піддавати її ризику.

Організаційні або адміністративні створюються на підприємствах в процесі створення та використання апаратури чи телекомунікаційних засобів для забезпечення безпеки. А саме будівництво приміщень, проектування систем, налаштування обладнання. Група цих засобів полягає в реалізації певних дій. Наприклад в обмежені доступу користувачів до приміщень з важливими ресурсами, розмежування доступу з наданням особливих прав невеликій кількості людей та забороні їм розповсюджувати будь-яку інформацію. Реалізація цих засобів здійснюється також через контроль за устаткуванням, забезпечення його роботи від додаткових генераторів.

Відключення станцій від локальних мереж під час обробки на них інформації.

Технічні засоби реалізуються за допомогою електричних, механічних, електромагнітних пристроїв, що перешкоджають проникненню та доступу до компонентів захисту та інформації. Розрізнять апаратні та фізичні засоби.

Апаратні – це пристрої, що встановлюються в використовувану апаратуру. Фізичні являють собою автономні пристрої та системи: замки, сигналізація.

Програмні засоби належать до спеціально створених захисних програм для захисту в каналах зв’язку. Наприклад, антивірусні, криптографічні, системи розмежування доступу.

Основна відмінність між бездротовими (*Wi-Fi*) та кабельними (*Ethernet*) мережами на рівні безпеки проявляється лише на перших двох рівнях мережевої моделі *OSI* – фізичному (*PHY*) та частково канальному (*MAC*). Вищі рівні, де реалізується основна частина механізмів безпеки, є спільними для обох типів мереж. Тому, якщо не приділити належної уваги налаштуванню безпеки бездротової мережі, зловмисники можуть отримати ряд несанкціонованих можливостей:

- Несанкціонований доступ до ресурсів: Зловмисник може проникнути в *Wi-Fi* мережу та отримати доступ до файлів, папок та інших ресурсів на комп'ютерах користувачів бездротової мережі, а в деяких випадках – і до ресурсів локальної дротової мережі (*LAN*), якщо вона підключена.
- Перехоплення трафіку (сніфінг): Зловмисник може прослуховувати бездротовий ефір та перехоплювати передані дані, включаючи конфіденційну інформацію, таку як паролі, номери кредитних карток, особисті повідомлення тощо.
- Маніпуляція даними: Зловмисник може не лише перехоплювати, але й спотворювати дані, що передаються в мережі, що може призвести до порушення працездатності систем або введення користувачів в оману.
- Нелегальне використання інтернет-трафіку: Зловмисник може використовувати чуже інтернет-з'єднання, що може призвести до збільшення витрат власника мережі або проблем з провайдером.
- Атаки на пристрої та сервери: Бездротова мережа може стати плацдармом для атак на комп'ютери користувачів (впровадження шкідливого програмного забезпечення) та сервери, підключені до мережі.
- Створення підроблених точок доступу (*Evil Twin*): Зловмисник може створити фальшиву *Wi-Fi* мережу з ідентичною назвою (*SSID*) до легітимної, щоб обманом змусити користувачів підключитися до неї та перехопити їхні дані.

• Зловмисні дії від імені мережі: Зловмисник, отримавши доступ до мережі, може використовувати її для розсилки спаму, здійснення *DDoS*-атак (розподілених атак на відмову в обслуговуванні) та інших незаконних дій, що може зашкодити репутації власника мережі.

На ранніх етапах розвитку *Wi-Fi* для обмеження доступу використовувався лише пароль *SSID* (ім'я мережі). Однак з часом стало очевидно, що цей метод не забезпечує достатнього рівня захисту, оскільки *SSID* передається у відкритому вигляді, і існують прості способи його перехоплення.

У стандарті *IEEE* 802.11 передбачені базові механізми для забезпечення безпеки бездротових мереж, включаючи аутентифікацію (процес перевірки легітимності пристрою для підключення до мережі) та шифрування (процес кодування даних для запобігання їхньому несанкціонованому перегляду). Сучасні стандарти безпеки *Wi-Fi*, такі як *WPA*3, використовують значно складніші та надійніші алгоритми аутентифікації та шифрування, ніж їхні попередники (*WEP*, *WPA*, *WPA*2), для ефективного захисту бездротових мереж від сучасних загроз.

2.2 Види загроз та вразливості бездротових комп’ютерних мереж

Загрози можна розділити за шкодою, яку вони завдають, на такі види:

- загроза порушення конфіденційності;

В основному направлені на розкриття і розповсюдження секретної інформації. Інша назва – несанкціонований доступ, тобто інформація стає відомою особам, що не мають на це право.

- порушення цілісності інформації;

Мета такої атаки змінити і порушити зміст інформації, що передається по мережі. Це може призвести до порушення якості або повного знищення інформації. Такі дії можуть нести направлений характер або бути наслідком впливів навколишнього середовища. Цей вид загрози є найпоширенішим для комп’ютерних мереж.

- порушення працездатності системи (відмова на обслуговування);

Порушення працездатності системи направлене на повне або часткове зупинення процесів обслуговування користувачів.

Атаки мають спеціальний та випадковий характер.

Інформація може зазнати впливу в будь-який цикл її життя. До випадкових можна віднести деякі помилки в апаратному та програмному забезпеченні, помилки операторів, відмови та збої в мережі, відключення живлення, перешкоди в лініях зв'язку через вплив навколишнього середовища.

Спеціальний характер передбачає умисне і цілеспрямоване завдання шкоди. Мотивами можуть бути бажання наживи, помста, завдання шкоди або просто цікавість.

Найпоширенішим проявом спеціального вторгнення є несанкціонований доступ (НСД). Суть цієї атаки полягає в отриманні прав доступу (перегляду, зміни, видалення) до інформації, в обхід правил розмежування доступу встановлених в даній системі. Здійснення НСД можливе при слабкій системі захисту. Для такої атаки використовуються самі робочі станції, канали зв'язку між ними, електромагнітне випромінювання від апаратури.

НСД може здійснюватись різними методами, такими як:

- перехоплення паролів, здійснюється спеціальними програмами для підміни реєстраційних форм або прослуховування каналу.

- "маскарад", виконання будь-яких дій від чужого імені, тобто від імені іншого користувача, передача повідомлень, вхід в систему.

- незаконне використовування повноважень, при розмежуванні повноважень кожен отримує відповідно до своєї посади. Від мінімальних до повних, при вході в систему від імені користувача з повними повноваженнями і завдати шкоди.

Виділяють пасивні та активні вторгнення в комп'ютерну мережу. При пасивному порушник для здійснення перехоплення інформації лише спостерігає за проходженням її по каналам зв'язку, прослуховує ("*sniffing*") не втручаючись в процес

передачі. Порушнику досить перебувати за сотні метрів від будівлі, в якій функціонує бездротова мережа, щоб виявити всі операції, що там відбуваються. Атакуючий може визначити довжину повідомлення, пункт направлення, а за допомогою накопичення та подальшого аналізу визначити захисні паролі, імена користувачів, номера кредитних карт. Для боротьби з цим видом атак достатньо створити ефективну систему шифрування інформації, що передається по від вузла до клієнта. В процесі шифрування біти змінюються за допомогою секретного ключа, що дає змогу приховати зміст повідомлень.

Активне втручання передбачає модифікацію та підміну інформації, зміну слідування або затримку повідомлень.

З поширенням мережі Інтернет розповсюдженими стають атаки на відстані. Атакуючий може знаходитися в будь-якій точці, головне щоб він мав доступ до Інтернету. Основний шлях впливу – програмний. Створено безліч програм для реалізації перехоплення, шпигунства, руйнування в інформаційних системах. Одна з таких програм “Троянський кінь” замаскована під корисну програму після запуску завдає значної шкоди системі безпеки мережі та комп’ютера: перехоплення паролів, знищення файлів, відповідальних за забезпечення безпеки системи.

Неавторизований доступ має в основі підключення будь-кого до закритої мережі. Якщо не реалізована система захисту, то зловмисник отримує доступ до усієї серверної та мережевої інформації.

Використовування базової конфігурації системи захисту не захищає від такого роду атак, оскільки в таких системах не передбачено надійного захисту при доступі до серверів мережі.

Користувач, що отримав доступ до мережі, може ознайомитись зі змістом будь-якого клієнта цієї мережі. Для запобігання цьому потрібно користуватися брандмауером.

Якщо в точці доступу реалізований певний захист, то існує загроза підключення до фіктивної точки доступу (*rogue access point*), яка зазвичай не авторизована і незахищена, і до якої доступ є значно легшим.

Співробітник або зловмисник може придбати точку доступу і підключити її до локальної мережі. Така точка доступу не має системи шифрування і дає змогу всім бажаючим підключитися до неї.

Для протидії фіктивним точкам доступу використовують метод взаємної аутентифікації. Аутентифікація – процес підтвердження справжності пристрою або користувача. Такі методи дозволяють користувачам та точкам доступу впевнетись у справжності один одного.

Точки доступу також повинні проходити процедуру аутентифікації на комутаторах, що виключає появу фіктивних точок доступу.

Атака типу “людина посередині” (*man in the middle attacks*) (див. рис. 2.1). Не зважаючи на систему захисту, хакери, знаючи як працюють мережеві протоколи, можуть легко виявити слабкі місця. Суть методу полягає в розміщенні фіктивного пристрою між легальними користувачами бездротової мережі. Зламник використовує протокол обробки адрес (*address resolution protocol, ARP*), який використовують всі мережі *TCP/IP*. За допомогою програмних засобів хакер може скористатись *ARP* і отримати контроль над бездротовою мережею.

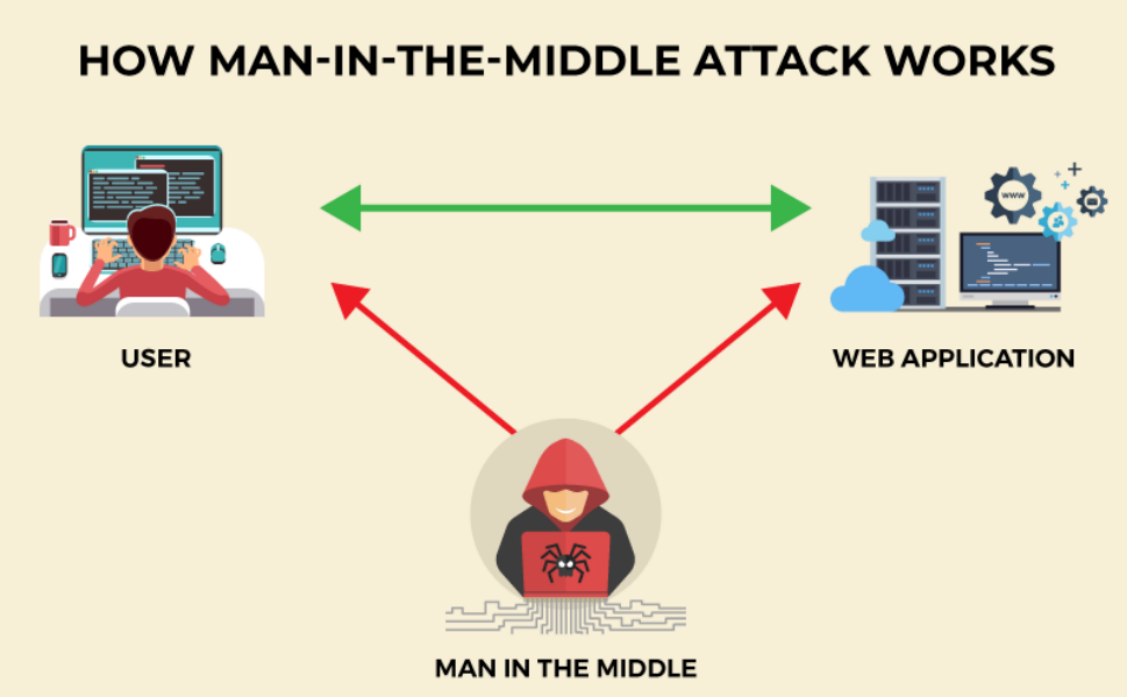

Рисунок 2.2 - Атака типу “людина посередині”

ARP дає можливість виявляти фізичну адресу мережевого адаптера, за допомогою запиту від адаптера. Адреса мережевої плати – це *MAC*- адреса, що є унікальною і назначається виробником. Плата-відправник мережевого інтерфейса реагує тільки на *MAC*- адресу плати-отримувача.

Передача здійснюється так: якщо потрібно передати дані, то відправник повинен мати *IP*-адреса отримувача. Тоді плата передавача використовуючи протокол *ARP* виконує пошук відповідної фізичної адреси. Це відбувається методом розсилання *ARP*- пакетів, в яких розголошується *IP*-адреса отримувача. Станція-отримувач впізнає себе та надсилає пакет-відповідь зі своїм *IP*-, *MAC*- адресами. Передавач включає *MAC*- адресу в фрейм передачі як адресу отримувача.

У бездротових мережах *Wi-Fi MAC*-адреси (*Media Access Control addresses*) передаються у фреймах даних у відкритому, незашифрованому вигляді. Це створює потенційну загрозу, оскільки зловмисники можуть перехоплювати ці адреси та використовувати їх для обходу деяких простих механізмів контролю доступу, таких як фільтрація *MAC*-адрес.

ARP протокол провокує *spoofing* – імітація з'єднання. Таким чином хакер може посилати фіктивні *ARP*-відповіді, що містять *IP*-адресу легітимного пристрою та *MAC*- адресу підставного. Це призводить до оновлення *ARP*- таблиць усіх станцій і вони починають передавати пакети нелегітимному пристрою. Хакер отримує можливість керувати сеансами зв'язку, він отримає паролі, доступ до інформації , а також можливість взаємодії з іншими серверами як легальний користувач.

Для запобігання атак цього типу виробники пропонують *ARP* з забезпеченням спеціального захищеного тунелю між кожним клієнтом і точкою доступу, який ігнорує всі непов'язані *ARP*-відповіді з клієнтом на іншому кінці тунелю.

Відмова обслуговування (*denial of service, DoS*) – атака, в наслідок якої мережа припиняє свою роботу. Це призводить до непередбачуваних наслідків ті збоїв у роботі мережі. Першим різновидом *DoS* атак є метод грубої сили (*brute force attack*). Реалізується за допомогою програм, що викликають інтенсивну передачу пакетів по мережі. Зламник може провести *DoS*-атаку шляхом відправки некорисних пакетів серверу з інших комп'ютерів мережі, що призводить до значного зниження як працездатності мережі так і її пропускної здатності.

Відомий спосіб зупинки роботи мережі, що використовує метод прослуховування несучої, шляхом потужного радіосигналу, що перекриває всі сигнали від точки доступу. Але такий напад можна виявити за допомогою засобів виявлення мережевих аналізаторів, оскільки хакер повинен знаходитись неподалік, щоб генерувати радіосигнал.

Інколи відмови обслуговування трапляються в мережі випадково. Через велике скупчення пристроїв: телефони, мікрохвильові печі, пристрої *Bluetooth* , що працюють в тому ж самому діапазоні частот, провокують зниження пропускної здатності мережі і появу великої кількості перешкод.

Хакери виявили слабкість в методі захищеного доступу до *Wi-Fi (Wi-Fi protected access, WPA)* і використовують її для атаки *DoS*. *WPA* користується математичним алгоритмом для аутентифікації користувачів в мережі. Якщо на протязі 1 секунди

відправити 2 пакети неавторизованих даних, то *WPA* вирішить, що став об'єктом атаки і припинить роботу мережі.

Основним захистом від атак такого типу є використання брандмауерів, постійно оновлені антивірусні засоби, використання надійних паролів, відключення від мережі не використовуваних пристроїв. Також можна забезпечити безпеку методом екранування приміщень ззовні.

2.3 Методи захисту *Wi-Fi* мереж

Wi-Fi мережі через свою бездротову природу несуть підвищені ризики безпеки порівняно з кабельною інфраструктурою. Зловмиснику не потрібно фізично підключатися до мережі – достатньо опинитися в зоні дії сигналу точки доступу.

Як ви вже зазначили, відмінності між бездротовими та дротовими мережами на рівні безпеки зосереджені переважно на фізичному (*PHY*) та канальному (*MAC*) рівнях моделі *OSI*. Саме на цих рівнях і виникають специфічні загрози для *Wi-Fi*, такі як:

- **Перехоплення трафіку (сніфінг):** Зловмисник може непомітно прослуховувати радіоефір та отримувати доступ до переданих даних.
- **Несанкціонований доступ:** Зловмисник може отримати доступ до мережевих ресурсів без належних облікових даних.
- **Дезінформація:** Зловмисник може втручатися в передачу даних, спотворюючи інформацію.
- **Атаки через підроблені точки доступу (*Evil Twin*):** Створення фальшивої *Wi-Fi* мережі для перехоплення облікових даних та трафіку користувачів.
- Інші види атак, такі як *DoS* (*Denial of Service*) або *Man-in-the-Middle*.

На початковому етапі розвитку *Wi-Fi* безпека обмежувалася простим паролем *SSID*, який виявився недостатнім для ефективного захисту.

Сьогодні для забезпечення безпеки бездротових мереж стандарту *IEEE* 802.11 застосовується комплексний підхід, що поєднує два ключові методи:

• **Шифрування (*Encryption*):** Процес кодування даних, що передаються бездротовим каналом, щоб зробити їх незрозумілими для сторонніх осіб, які можуть перехопити сигнал. Сучасні стандарти шифрування, такі як *AES* (*Advanced Encryption Standard*), що використовуються в *WPA*3, забезпечують високий рівень захисту.

• **Аутентифікація (*Authentication*):** Процес перевірки особистості користувача або пристрою, який намагається підключитися до бездротової мережі. Сучасні методи аутентифікації, наприклад *WPA*3-*Enterprise*, використовують складніші протоколи для забезпечення надійного контролю доступу.

Таким чином, сучасні бездротові мережі мають значно потужніші інструменти безпеки порівняно з ранніми реалізаціями, але правильне налаштування та використання цих інструментів залишається критично важливим для захисту від потенційних загроз.

Криптографія – наука про методи перетворення даних, при якій вони стають незрозумілі і некорисні для зламника. Зміни інформації перешкоджають несанкціонованому доступу, вилученню інформації при прослуховуванні каналу зв'язку (вирішується проблема конфіденційності) та змоги змінити чи знищити інформацію (вирішення проблеми цілісності даних).

Текст, генерований відправником називається відкритим текстом, а текст, зашифрований по одному з алгоритмів – криптограма або шифр-текст.

Криптоаналіз – наука про розкриття відкритого тексту зашифрованого повідомлення без доступу до ключа. В результаті аналізу може бути розкрито вхідний текст або секретний ключ, а також сприяє виявленню слабких місць в криптосистемі.

Шифрування: Захист даних за допомогою ключів

Ключ у криптографії – це секретний набір параметрів, який визначає унікальний спосіб шифрування та розшифрування даних за певним алгоритмом. Криптостійкість шифру визначає його здатність протистояти криптоаналізу – спробам розшифрувати дані без знання ключа. Чим більший час і обчислювальні ресурси потрібні для злому шифру, тим вища його криптостійкість.

Будь-яка спроба зловмисника отримати оригінальний текст із зашифрованого без знання секретного ключа називається криптоаналітичною атакою. Криптосистема вважається криптостійкою, якщо всі такі спроби є невдалими.

До сучасних шифрів, що використовуються для захисту інформації, висуваються такі основні вимоги:

- Висока криптостійкість, що відповідає рівню загроз.
- Ефективні та швидкі алгоритми шифрування та розшифрування.
- Мінімальне збільшення обсягу даних після шифрування.
- Стійкість до незначних помилок у процесі шифрування.

Історично використовувалися різні типи шифрів, такі як перестанови, заміни та гамування. Сучасні криптосистеми часто використовують аналітичні перетворення даних, наприклад, математичні функції та матричні операції.

Процеси шифрування та розшифрування відбуваються в рамках певної криптосистеми, які поділяються на два основні класи:

- Симетричні (одноключові) криптосистеми: Використовують один і той самий секретний ключ як для шифрування, так і для розшифрування даних. Ключ необхідно безпечно передати між відправником та отримувачем. Прикладами є *DES, AES* та *RC*4 (хоча останній вважається застарілим для безпечного використання).
- Асиметричні (двохключові) криптосистеми (з відкритим ключем): Використовують пару ключів – відкритий ключ для шифрування (доступний для всіх) та приватний (секретний) ключ для розшифрування (відомий лише отримувачу). Розшифрування за допомогою відкритого ключа неможливе. Прикладами є *RSA* та *ECC*.

Механізми шифрування часто використовують алгоритми рандомізації даних для підвищення їхньої безпеки.

Розрізняють два основні типи шифрів за способом обробки даних:

- Потокові шифри: Генерують безперервний ключовий потік, який комбінується з відкритим текстом для отримання шифротексту. *RC*4 був прикладом потокового шифру, але через виявлені вразливості його не рекомендується використовувати.
- Блокові шифри: Обробляють дані фіксованими блоками. Відкритий текст розбивається на блоки, і кожен блок шифрується незалежно за допомогою ключового потоку фіксованого розміру. *AES* є сучасним та надійним блоковим шифром.

Режим шифрування, при якому кожен однаковий блок відкритого тексту шифрується в однаковий блок шифротексту (*Electronic Code Book, ECB*), є вразливим до криптоаналізу. Для підвищення безпеки використовуються вектори ініціалізації (*IV*) та режими зі зворотним зв'язком (наприклад, *CBC*, *CTR*), які забезпечують унікальне шифрування однакових блоків відкритого тексту. Вектор ініціалізації – це випадкове або псевдовипадкове число, яке додається до ключа для кожного сеансу шифрування, забезпечуючи різне шифрування однакових даних.

Застарілий стандарт *WEP* (*Wired Equivalent Privacy*):

Стандарт *IEEE* 802.11 колись передбачав захист за допомогою алгоритму *WEP*, який використовував симетричний потоковий шифр *RC*4 зі статичними ключами довжиною 40 або 104 біти та 24-бітним вектором ініціалізації. Однак *WEP* виявився вкрай вразливим через повторне використання векторів ініціалізації, що дозволяло зловмисникам відносно швидко зламувати ключ. Тому *WEP* на сьогоднішній день вважається ненадійним і не повинен використовуватися.

Сучасні стандарти безпеки:

Після виявлення вразливостей *WEP* були розроблені значно надійніші стандарти безпеки:

- *IEEE* 802.1*X*: Стандарт для контролю доступу до мережі, що використовує динамічні ключі шифрування та протокол розширеної аутентифікації (*EAP*).
- *WPA* (*Wi-Fi Protected Access*): Тимчасовий стандарт, що поєднував динамічне оновлення ключів (*TKIP*), протокол *EAP* та перевірку цілісності повідомлень (*MIC*), щоб усунути недоліки *WEP*.

- *WPA*2 (*Wi-Fi Protected Access* 2) / *IEEE* 802.11*i*: Надійніший стандарт, який замінив *TKIP* на більш безпечний алгоритм шифрування *AES*. *WPA*2 пропонує режими *PSK* (*Pre-Shared Key*) для домашніх і малих офісів та 802.1*X* для корпоративних мереж з використанням сервера аутентифікації.
- *WPA*3 (*Wi-Fi Protected Access* 3): Найсучасніший стандарт безпеки, що забезпечує ще вищий рівень захисту завдяки новим протоколам аутентифікації (*SAE*) та шифрування (*GCMP*-256).

VPN (*Virtual Private Network*): Технологія, яка створює зашифрований "тунель" через загальнодоступні мережі (наприклад, інтернет) для безпечного підключення клієнтів до мережі або сервера. *VPN* забезпечує конфіденційність та цілісність даних, часто використовуючи протокол *IPSec*. *VPN* вважається одним з найнадійніших способів захисту мережевого трафіку.

Додаткові методи захисту бездротових мереж:

- Заборона віддаленого керування точкою доступу через *Wi-Fi*: Обмеження доступу до налаштувань роутера лише через дротове з'єднання.
- Фільтрація за *MAC*-адресами: Дозволяє доступ до мережі лише пристроям з попередньо визначеними *MAC*-адресами (хоча цей метод легко обійти).
- Приховування *SSID*: Запобігає відображенню назви мережі у списку доступних *Wi-Fi* мереж (лише ускладнює виявлення, але не є надійним захистом).
- Розташування обладнання: Розміщення антен подалі від зовнішніх стін та вікон, а також обмеження потужності сигналу може зменшити радіус дії мережі.
- Використання складних та довгих паролів/ключів: Ускладнює їхнє вгадування або злам.
- Регулярна зміна статичних ключів та паролів.
- Обмеження використання протоколу *TCP*/*IP* для спільного доступу до файлів та принтерів у бездротовій мережі.
- Використання складних паролів для гостьового доступу (за потреби).

- Використання статичних *IP*-адрес замість *DHCP*: Ускладнює підключення неавторизованих пристроїв (але не є основним методом захисту).
- Встановлення файєрволів на всіх пристроях у бездротовій мережі та на точці доступу.
- Обмеження кількості використовуваних протоколів у *WLAN* (наприклад, лише *HTTP* та *SMTP*).
- Регулярне сканування мережі на наявність вразливостей за допомогою спеціалізованих інструментів.
- Використання захищених мережевих операційних систем.

Важливо пам'ятати, що людський фактор залишається однією з основних загроз безпеці мережі. Недбалість у налаштуваннях, використання слабких паролів або розголошення конфіденційної інформації можуть звести нанівець навіть найсучасніші технології захисту.

Аутентифікація: Перевірка особистості користувача

Системи ідентифікації та аутентифікації використовуються для контролю доступу до мережевих ресурсів.

- Ідентифікація: Процес розпізнавання користувача за його унікальним ідентифікатором (наприклад, логіном).
- Аутентифікація: Процес перевірки справжності ідентифікатора користувача за допомогою секретної інформації (пароль, ключ, біометричні дані тощо).
- Авторизація: Процес визначення прав та дозволів користувача після успішної аутентифікації.

Стандарт *IEEE* 802.11 передбачає два основні механізми аутентифікації:

- Відкрита аутентифікація (*Open Authentication*): Фактично відсутність аутентифікації. Точка доступу приймає будь-який запит на підключення, якщо правильно налаштовані *WEP*-ключі (якщо використовуються). Будь-який пристрій, що знає *SSID*, може підключитися. Цей метод є небезпечним, якщо не використовуються надійніші методи шифрування на вищих рівнях.

• Аутентифікація зі спільним ключем (*Shared Key Authentication*): Вимагає наявності однакових *WEP*-ключів на точці доступу та клієнті. Клієнт повинен правильно зашифрувати текст виклику, отриманий від точки доступу, щоб бути аутентифікованим. Цей метод також вважається вразливим через передачу ключів у зашифрованому, але все ж таки перехоплюваному вигляді.

Для забезпечення більш високого рівня безпеки в бездротових мережах важливо використовувати взаємну аутентифікацію, при якій перевіряється ідентичність як клієнта, так і точки доступу. Це допомагає запобігти атакам з використанням підроблених точок доступу. Для цього часто використовуються сервери аутентифікації, такі як *RADIUS*.

Стандарт *IEEE* 802.1*X* дозволяє налаштувати автоматизовану систему аутентифікації та контролю трафіку, використовуючи протокол *EAP*, який підтримує різні методи аутентифікації, включаючи паролі, сертифікати та одноразові паролі. У моделі 802.1*X* клієнт (*supplicant*) намагається підключитися до аутентифікатора (точка доступу), який перенаправляє запити на сервер аутентифікації (*RADIUS*). До успішної аутентифікації трафік клієнта блокується.

Таким чином, сучасні бездротові мережі мають потужні засоби захисту, але їхня ефективність залежить від правильної конфігурації та обізнаності користувачів та адміністраторів щодо потенційних загроз та методів їхнього запобігання.

2.4 Віртуальні приватні мережі

За останнє десятиліття бурхливий розвиток інтернету та публічних мереж *Wi-Fi* кардинально змінив інформаційний простір, зокрема питання безпеки та доступу до даних. Користувачі отримали дешеві та зручні канали зв'язку, а бізнес, прагнучи оптимізувати витрати, часто передає комерційну інформацію через ці потенційно незахищені середовища. Проте сама архітектура бездротових мереж створює для зловмисників можливості перехоплення, модифікації або викрадення даних.

Для ефективної протидії кіберзагрозам та забезпечення безпечної роботи в публічних мережах на початку 90-х років виникла концепція віртуальних приватних мереж (*VPN*).

В основі *VPN* лежить ідея створення зашифрованого "тунелю" між двома або більше вузлами в глобальній мережі (наприклад, в інтернеті) для забезпечення конфіденційності та цілісності обміну даними. Доступ до цього віртуального каналу є неможливим для сторонніх спостерігачів. Важливо, що цей тунель не є постійним, а встановлюється лише на час передачі трафіку.

VPN (*Virtual Private Network*) – це технологія, яка об'єднує локальні мережі та окремі комп'ютери через публічну мережу в єдину захищену віртуальну корпоративну мережу, гарантуючи безпеку переданої інформації.

Підключення локальної мережі до відкритої мережі завжди несе ризики несанкціонованого вторгнення, зміни або викрадення даних. Захист інформації в таких сценаріях базується на аутентифікації сторін, що взаємодіють, криптографічному шифруванні даних та перевірці цілісності отриманої інформації.

Для захисту мережі та її компонентів від зовнішніх загроз використовуються міжмережеві екрани (*firewalls*). Вони забезпечують безпеку, фільтруючи вхідний та вихідний мережевий трафік, а також можуть виступати в ролі посередників при обміні даними. Міжмережеві екрани встановлюються на межі між локальною та публічною мережами. Для захисту окремих віддалених комп'ютерів використовуються персональні міжмережеві екрани, встановлені безпосередньо на цих пристроях.

Основу захисту даних при передачі через публічні канали становить створення захищених віртуальних каналів зв'язку – криптозахищених тунелів. Тунель – це логічне з'єднання, що проходить через відкриту мережу, по якому передаються зашифровані пакети даних. За створення тунелю відповідають *VPN*-клієнт та *VPN*-сервер (або два *VPN*-маршрутизатори), які виступають як ініціатор та термінатор тунелю. Ініціатор тунелює (інкапсулює) оригінальні пакети даних у нові пакети, додаючи заголовки з інформацією про відправника та отримувача *VPN*-з'єднання.

Хоча всі пакети, що передаються через тунель, є *IP*-пакетами, інкапсульовані пакети можуть належати до різних мережевих протоколів. Маршрут між ініціатором та термінатором визначається звичайною *IP*-маршрутизацією. Термінатор виконує зворотний процес – декапсуляцію, видаляючи додаткові заголовки та направляючи оригінальні пакети до локального стеку протоколів або до кінцевого адресата в локальній мережі.

Сама інкапсуляція не забезпечує захист даних. Безпека досягається завдяки криптографічному захисту інкапсульованих пакетів. Конфіденційність забезпечується шифруванням, а цілісність та автентичність – використанням цифрових підписів.

Для успішної роботи *VPN* критично важливими є:

- Використання ініціатором та термінатором сумісних методів шифрування та можливість автоматичного узгодження цих параметрів.
- Підтримка безпечного обміну ключами шифрування для забезпечення можливості розшифрування даних та перевірки цифрових підписів.
- Аутентифікація граничних пристроїв тунелю для гарантування встановлення з'єднання між авторизованими користувачами.

Віртуальні приватні мережі класифікуються за кількома ознаками:

- Рівень моделі *OSI*: *VPN* можуть працювати на канальному (*Layer* 2), мережевому (*Layer* 3) або сеансовому (*Layer* 5) рівнях. Вибір рівня впливає на функціональність, прозорість для додатків та сумісність з іншими засобами захисту. *VPN*, що працюють на нижчих рівнях, як правило, є більш прозорими для додатків.
- Конфігурація структурно-технічного рішення: Розрізняють *VPN* з віддаленим доступом (*Remote Access*), внутрішньокорпоративні *VPN* (*Intranet VPN*) та міжкорпоративні *VPN* (*Extranet VPN*).
- Спосіб технічної реалізації: *VPN* можуть бути реалізовані на основі мережевих операційних систем, міжмережевих екранів, маршрутизаторів, програмних рішень або спеціалізованих апаратних засобів.

Класифікація *VPN* за рівнем *OSI*:

Технологію безпечної передачі даних через публічну мережу часто називають захищеним каналом (*secure channel*). *VPN* можуть бути реалізовані на різних рівнях *OSI*, що визначає їхню функціональність та сумісність.

- *VPN* канального рівня (*Layer* 2 *VPN*): Забезпечують інкапсуляцію різних видів трафіку та створення віртуальних тунелів "точка-точка" (наприклад, між маршрутизаторами або між комп'ютером та шлюзом). До цієї групи належать протоколи *L2F*, *PPTP* та *L2TP*. *PPTP* забезпечує прозорість для додатків, а *L2TP* часто використовується для віддаленого доступу.
- *VPN* мережевого рівня (*Layer* 3 *VPN*): Інкапсулюють *IP*-пакети в *IP*-пакети. Протоколом цього рівня є *IPSec*, який забезпечує аутентифікацію, тунелювання та шифрування *IP*-трафіку. *IPSec* є прозорим для більшості додатків та може працювати в різних мережах. Протокол *IKE* відповідає за безпечне управління та обмін ключами шифрування в *IPSec*.
- *VPN* сеансового рівня (*Layer* 5 *VPN*): Використовують "посередники каналів" (*circuit proxy*), що працюють над транспортним рівнем. Трафік з захищеної мережі ретранслюється в інтернет для кожного сокету окремо. Шифрування часто реалізується за допомогою *TLS*. Протокол *SOCKS* (особливо версія 5) стандартизує аутентифікований прохід через міжмережеві екрани в цьому режимі.

Класифікація *VPN* за архітектурою:

- *VPN* з віддаленим доступом (*Remote Access VPN*): Забезпечують безпечний віддалений доступ до корпоративних ресурсів для мобільних та віддалених співробітників.
- Внутрішньокорпоративні *VPN* (*Intranet VPN*): Забезпечують захищену взаємодію між підрозділами всередині компанії або між групами підприємств, об'єднаних корпоративними мережами.

- Міжкорпоративні *VPN* (*Extranet VPN*): Забезпечують захищений обмін інформацією зі стратегічними партнерами, надаючи прямий доступ між мережами різних компаній з контролем доступу та аутентифікацією.

Класифікація *VPN* за способом реалізації:

- *VPN* на основі мережевої операційної системи: Економічний варіант, але може мати обмежену безпеку (наприклад, *PPTP*).
- *VPN* на основі маршрутизаторів: Маршрутизатор виконує функції маршрутизації та шифрування.
- *VPN* на основі міжмережевих екранів: Міжмережевий екран доповнюється функціями тунелювання та шифрування. Вартість може бути вищою, а продуктивність залежить від апаратного забезпечення.
- *VPN* на основі програмного забезпечення: Спеціалізоване програмне забезпечення на віддаленому комп'ютері виконує функції *VPN*-клієнта або проксі-сервера.
- *VPN* на основі спеціалізованих апаратних засобів з вбудованими шифропроцесорами: Забезпечують високу продуктивність, але є найдорожчим варіантом.

Технологія *VPN* є ефективним рішенням для захисту конфіденційної інформації, що передається через незахищені канали зв'язку. Вона забезпечує безпечний зв'язок між мережами, їхніми компонентами та віддаленими користувачами через зашифрований тунель в інтернеті. Завдяки своїй відносній дешевизні та надійності, використання *VPN* стає все більш актуальним та поширеним, забезпечуючи продуктивність, оперативність, захищеність та цінову доступність для обміну інформацією. Очікується подальший розвиток та масове впровадження *VPN*-технологій.

РОЗДІЛ 3
ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ *WI-FI*

3.1 Загальна структура мережі

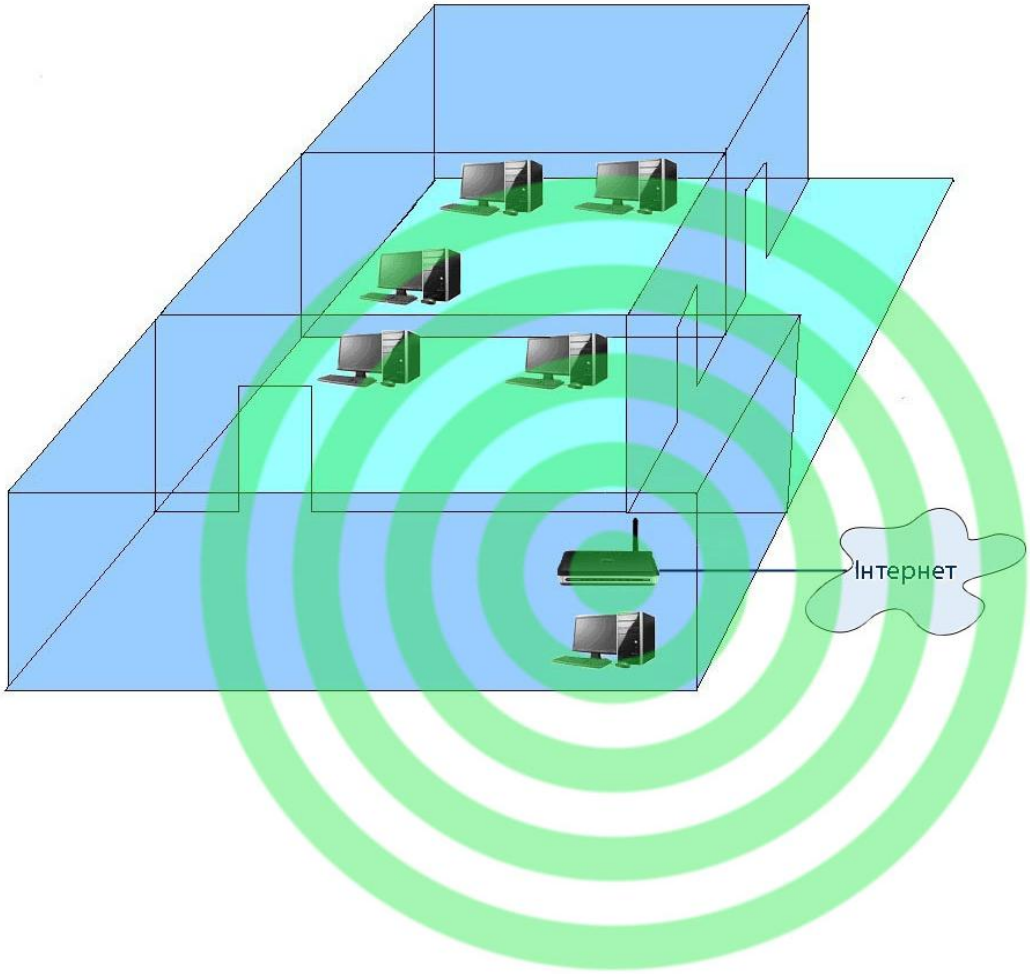

Рисунок 3.1 - План-схема мережі

Мережа (див. рис. 3.1) розміщена на одному поверсі та займає три кімнати. До її складу входять шість комп'ютерів та точка доступу – бездротовий маршрутизатор, що має мережний інтерфейс (*uplink port*). Через цей інтерфейс здійснюється налаштування точки. Точка доступу підключена до мережі Інтернет.

Бездротовий маршрутизатор знаходиться в кабінеті директора і з'єднаний з іншими станціями в інфраструктурному режимі.

Доступ до мережі забезпечується шляхом передачі широкомовних сигналів через ефір у частотному діапазоні 2,4 Ггц. Мережеве обладнання підтримує стандарти *Wi-Fi* 802.11*b* та 802.11*g*.

Всі комп'ютери оснащені бездротовими адаптерами, які підключаються через слот розширення *PCI*.

Основним призначенням мережі є можливість передавати документи для обробки на інщі комп'ютери мережі та забезпечувати доступ до мережі Інтернет.

3.2 Проектування системи захисту бездротової мережі

Оскільки точка доступу знаходиться у крайній кімнаті, то розповсюдження сигналу виходить далеко за межі офісу і виникає потреба у розробці ефективної системи безпеки для захисту від вторгнень та крадіжки важливої фінансової інформації.

До нашої незахищеної мережі може підключитися будь-хто цікавий та заподіяти значної шкоди виробничому процесу або безкоштовно використовувати Інтернет ресурси для розповсюдження спаму та вірусів. І вся відповідальність буде покладена на фірму.

Окрім обов'язкової зміни пароля доступу до налаштувань *Wi-Fi* точки, для захисту бездротової мережі ми будемо використовувати наступні заходи:

Фільтрація за *MAC*- адресами.

Використовуючи налаштування точки доступу ми заборонимо підключення до бездротової мережі усіх комп'ютерів , окрім тих, які ми занесемо в спеціальний список дозволів - *Access List* (див. рис. 3.2). Цей метод захисту заснований на тому, що кожна мережева карта комп'ютера має свій власний номер наданий їй при

виробництві. Дізнатися цей номер та підробити його дуже легко , але цим ми можемо забезпечити тимчасову перешкоду на шляху зловмисника.

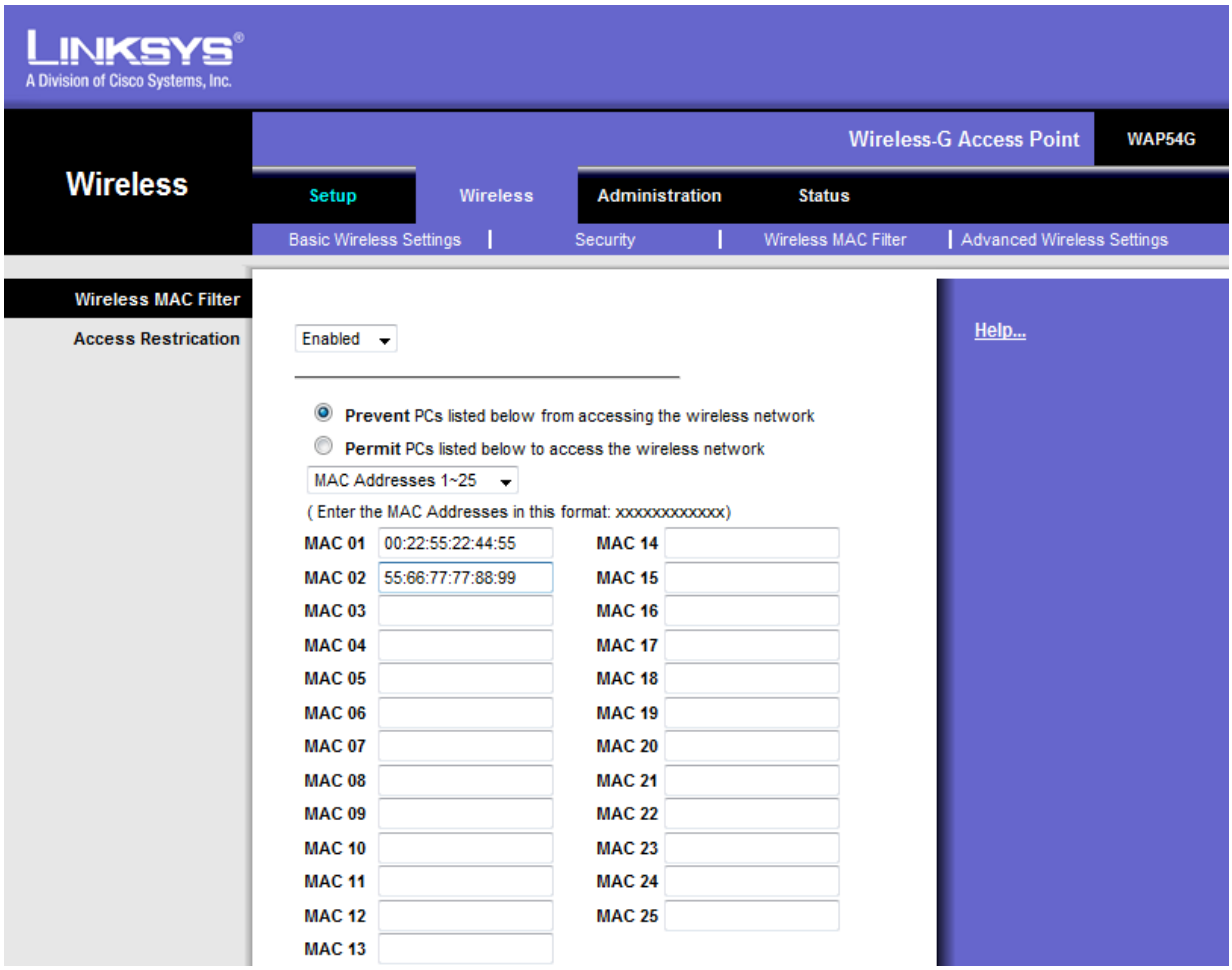

Рисунок 3.2 - Список дозволених *MAC*- адрес

Використання *WPA3-Enterprise* (див. рис. 3.3).

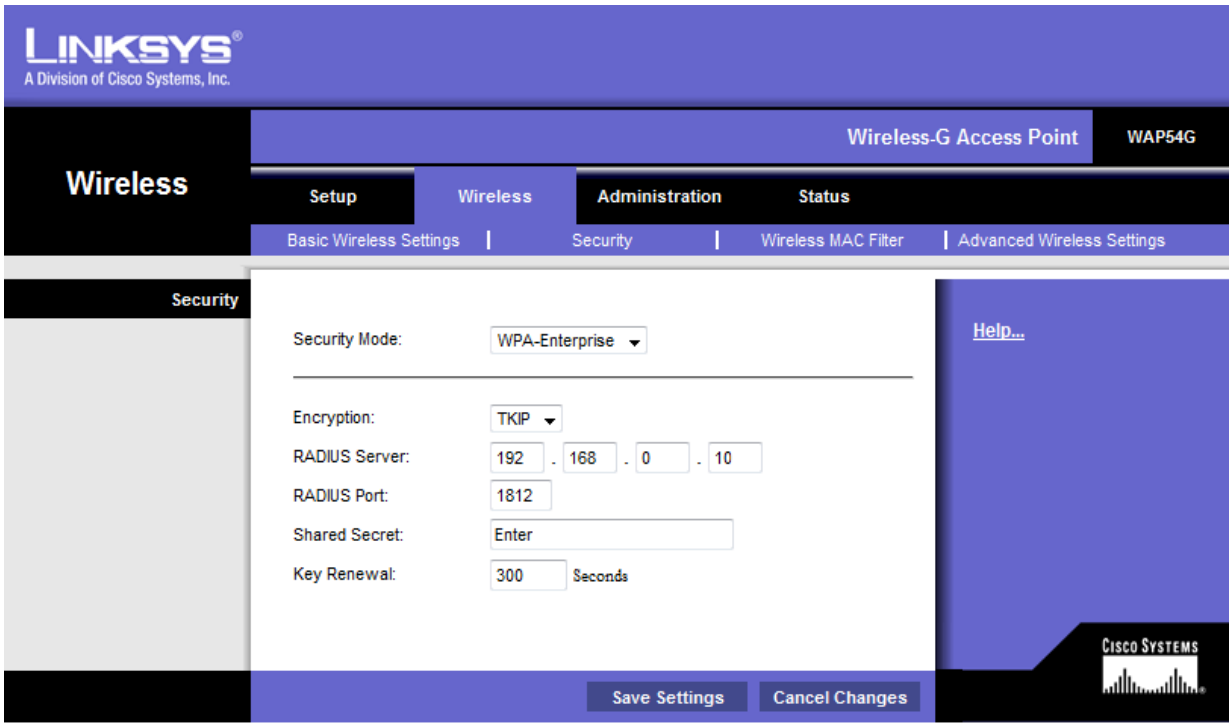

Рисунок 3.3 - Вікно налаштувань *WPA3-Enterprise*

Для забезпечення цієї схеми захисту бездротової мережі окрім правильно налаштованої точки доступу, ми будемо використовувати ще один комп'ютер.

Цей комп'ютер буде виконувати роль сервера аутентифікації - *RADIUS*-сервера. Для організації сервера можна використовувати будь-який старий комп'ютер.

Він буде перевіряти справжність користувачів, які намагатимуться отримати доступ до мережі. Перевірка ведеться за допомогою логіна та пароля або по цифровим сертифікатам. Цифровий сертифікат – це спеціальний файл, що зберігається на *RADIUS*-сервері та на клієнтській станції. При спробі підключення до мережі сертифікати звіряються і у випадку спів падіння надається доступ до мережі. А за допомогою кореневого сертифіката відбувається перевірка справжності сервера.

Використання *RADIUS*-сервера дає дуже високий ступінь захисту.

Щоб організувати *RADIUS*-сервер для нашої мережі ми будемо використовувати окремий комп'ютер з двома мережевими картами , на який встановимо програмний маршрутизатор *Esomo*. До складу *Esomo* входить операційна система - *FreeBSD*.

Esomo також може вести облік трафіку для кожного користувача та дозволяти доступ до Інтернету з унікальним логіном та паролем.

Під час встановлення *FreeBSD Esomo* вся інформація на жорсткому диску комп'ютера буде стерта. Для встановлення операційної системи нам потрібно буде на деякий час під'єднати монітор та клавіатуру, які в подальшому для сервера не знадобляться.

Першу мережеву карту ми підключимо до Інтернет кабеля, а іншу до бездротового маршрутизатора.

Вставимо диск з образом *Esomo* в дисковод та перезапустимо систему, встановивши в *BIOS* загрузку с *CD*. Після перезапуску розпочнеться встановлення *Esomo*. В ході установки треба звернути увагу на правильність вказаних мережевих установок.

Ім'я хосту – ім'я комп'ютера з *Esomo*, вводиться на англійській мові.

Пароль адміністратора – пароль для входу в операційної систему *FreeBSD*, повинен містити лише англійські літери та цифри. В цілях безпеки пароль краще вказати.

Внутрішню *IP*- адресу *Esomo* – *IP* адресу комп'ютера з *Esomo* в нашій мережі. Ми введемо 192.168.0.1 , а маску під мережі залишимо як є – 255.255.255.0 .

Зовнішня *IP*- адреса *Esomo* – адреса назначена Інтернет провайдером.

Натиснемо «Далі» , а в наступному вікні «*Yes*» для продовження інсталяції *Esomo* на комп'ютер. Після завершення ми побачимо вікно з інструкціями, які потрібно записати та натиснемо «*OK*». У вікні з попередженням про перезапуск системи натиснемо «*OK*».

Тепер за допомогою витої пари тимчасово з'єднаємо робочий комп'ютер та сервер з *Esomo*. Через 5 хвилин на своєму робочому комп'ютері зайдемо в «Пуск» - «Виконати» і введемо *cmd*. У вікні, що з'явилося , наберемо «*ping* 192.168.0.1» та натиснемо «*Enter*» (див. рис. 3.4). Повинна з'явитись відповідь від комп'ютера з

Esomo. Якщо відповіді немає , то переставте кабель в іншу мережеву карту комп'ютера з *Esomo*.

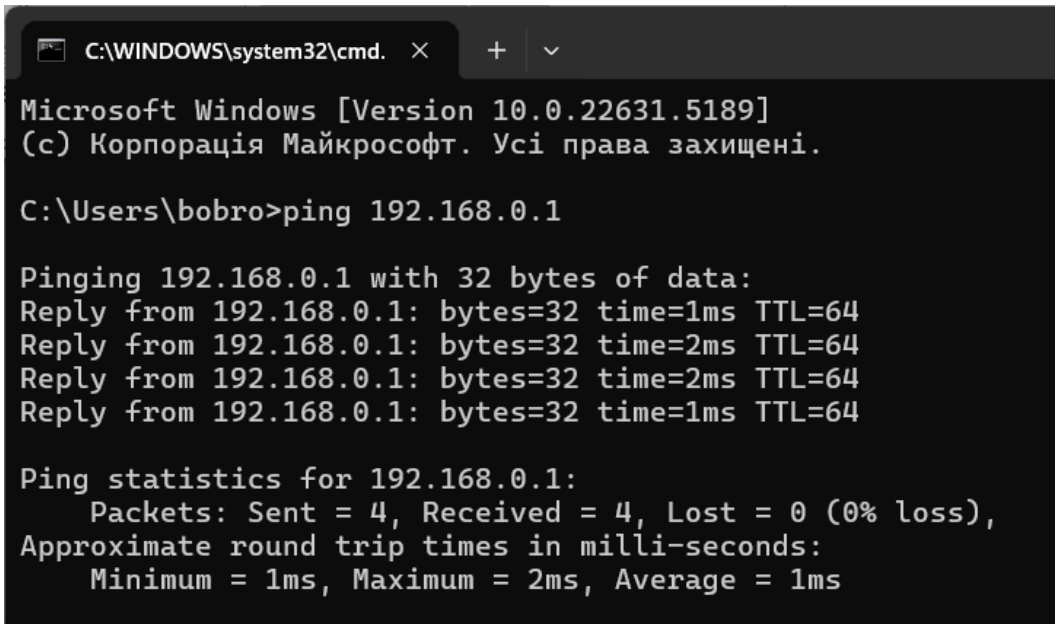

Рисунок 3.4 - Виконання команди «*ping* 192.168.0.1»

Максимальний захист бездротового трафіку в мережі з *Esomo* досягається за рахунок використання технології *VPN* у поєднанні зі встановленим бездротовим з'єднанням по протоколу *WPA*, що забезпечує другий рівень шифрування трафіку. Створення *VPN*- з'єднання між користувачем та сервером з *Esomo* відбувається автоматично.

Отримавши відповідь від комп'ютера з *Esomo*, у строці адреси браузера наберемо «*http*://192.168.0.1/».

Нам буде запропоновано встановити компонент *ActiveX*. Дозволимо завантаження та встановлення цього компоненту. Через деякий час з'явиться вікно для вводу логіна та пароля. Введемо пароль та логін і натиснемо «З'єднати».

Між нашим комп'ютером та *Esomo* буде встановлено віртуальне з'єднання з шифруванням трафіку.

За допомогою правої кнопки миші та контекстного меню створимо ярлик для цього з'єднання та виведемо його на Робочий стіл, щоб в подальшому підключатися до сервера без відкриття браузера.

Тепер можна перейти до налаштувань *Esomo* для роботи з бездротовою мережею.

На диску з *Esomo* знайдемо каталог *Win* та скопіюємо його собі на комп'ютер. Знайдемо в папці *Win* файл *Esomo.exe* та запустимо його, введемо в поля логін та пароль. З'явиться вікно програми *APM* – це спеціальна програма , яка дозволяє робити налаштування з *Esomo* за допомогою мережі.

Оскільки *Esomo* буде рахувати використаний трафік, додамо новий тариф.

У розділі «Тарифи» натиснемо кнопку «Додати» , введемо назву тарифу та ціну -1 , як для безлімітного Інтернету.

Тепер додаємо користувачів, що будуть підключатися до нашої мережі та користуватися Інтернетом. Для кожного користувача створимо окремий обліковий запис.

Додавати нових користувачів будемо в розділі «Користувачі».

Користувачів можна об'єднувати в групи: для цього спочатку додамо нову групу, виділимо її мишкою потім додаємо в групу потрібних користувачів.

При додаванні облікових записів Інтернет користувачів помітки в розділі «Права» не ставляться.

Обліковий запис адміністратора має права на конфігурацію програми. Помітки в полях «Права» ставляться, оскільки адміністратору не потрібен Інтернет, а лише можливість налаштування програми.

Операція поповнення рахунку Інтернет – користувача.

Виділимо користувача та на панелі інструментів натиснемо «Додати платіж». Введемо суму та джерело оплати.

Перейдемо до налаштувань *Esomo* та конфігурування точки доступу.

Перевіримо опції динамічного розподілення *IP* адрес у *Esomo*. Для цього в розділі «Настройки сервера» відкриємо вкладку «*DHCP*» і перевіримо чи стоїть мітка

навпроти «Увімкнути динамічний *DHCP*». Ця опція забезпечить автоматичне присвоєння *IP* адрес точці доступу та комп'ютерам *Wi-Fi* мережі.

В таблиці «Статичний *DHCP*» натиснемо «Додати» та додамо дані нашої точки доступу.

MAC – адреса міститься в документації до точки доступу, *IP* адреса точки доступу та ім'я точки доступу на англійській мові. В *IP* адресі точки доступу перші три цифри повинні співпадати з відповідними *IP* адреси внутрішнього мережевого інтерфейсу комп'ютера з *Esomo*. Ім'я – будь-яке.

Натиснемо «Застосувати». З'єднання з *Esomo* буде розірвано і, щоб відновити його, ми клацнемо по ярлику на Робочому столі.

Перейдемо в розділ «*Wi-Fi*» і на вкладці «Точки доступа» додамо нашу бездротову точку доступу в список. Вкажемо ім'я, а *IP* адреса буде така ж, як і в попередньому вікні. Ключ – кодову слово на англійській мові , по якому точка доступу та сервер *Esomo* впізнають один одного. Цей ключ пізніше ми вкажемо в налаштуваннях точки доступу. Після введення всіх даних натиснемо «Застосувати». Знову відновимо втрачене з'єднання з *Esomo*.

Забезпечимо кожного користувача мережі цифровим сертифікатом. Для цього перейдемо в розділ «*Wi-Fi*» на вкладку «Сертифікати». Клацнемо правою клавішею миші по імені користувача та оберемо опцію «Згенерувати користувацький сертифікат» , введемо кількість днів дії сертифіката та натиснемо «ОК».

Esomo APM запропонує вам зберегти створені цифрові сертифікати для користувача та кореневий сертифікат. Оберіть місце на диску та збережіть.

Згенеруємо цифрові сертифікати для всіх користувачів мережі. Поряд зі значком сертифіката буду відображатися строк його дії. По закінчені цього терміну користувачі не зможуть підключитися до мережі. Кореневий сертифікат є однаковим для всіх користувачів. Достатньо зберегти його один раз і використовувати надалі. На цьому налаштування *Esomo* завершено.

Тепер налаштуємо точку доступу (див. рис. 3.5). Під'єднаємо маршрутизатор до комп'ютера. Відкриємо браузер та наберемо у адресній строці *IP* адресу точки доступу. Він має бути вказаний в документації.

Після підключення до *Wi-Fi* точки доступу та вводу логіна і пароля доступу ми потрапляємо в утиліту для її налаштування. Точка доступу завжди доступна через *Web* інтерфейс.

Для підвищення рівня безпеки ми змінемо стандартні логін та пароль, щоб ускладнити доступ до налаштувань зловмисникам. Ідеальний пароль може бути довжиною 128-256 біт та складатися зі строчних та заглавних літер, містити цифри та спеціальні знаки, наприклад - o*R*23@&_2*kL*/ .

Для бездротової точки доступу ми вкажемо наступні налаштування:

- динамічне отримання *IP* адреси від *Esomo* або статичну адресу, яку ми вказали в мережевих налаштуваннях на вкладці «*DHCP*». У нас це 192.168.0.9. шлюзом для точки доступу буде комп'ютер з *Esomo* – 192.168.0.1.

- ім'я точки доступу, що ми обрали та вказали на вкладці «*DHCP*» і в розділі «*Wi-Fi*» *Esomo APM*. У нас це – *linksys*.

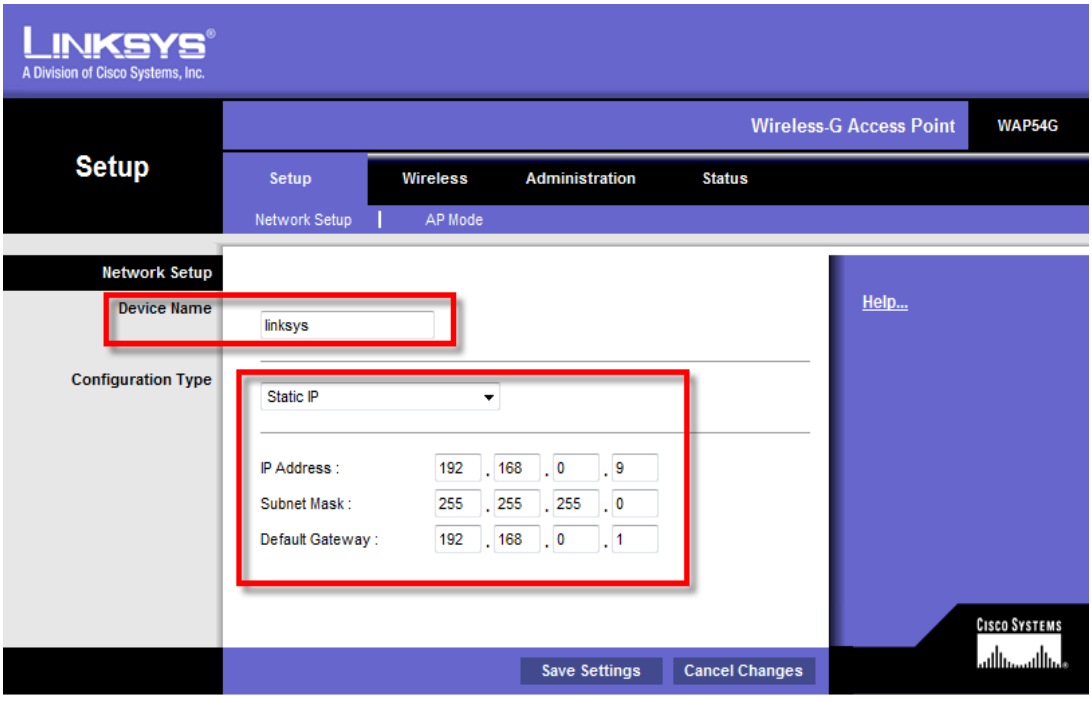

Рисунок 3.5 - Вікно налаштувань точки доступу

- ім’я нашої бездротової мережі або *SSID* (ідентифікатор мережі) (див. рис. 3.6).

SSID є важливим параметром для отримання доступу до мережі. Зазвичай *SSID* передається в ефір в широкомовному режимі і це становить певну загрозу для мережі – бути виявленою зламником. Щоб уникнути цього ми відключємо широкомовну трансляцію *SSID* в ефір. Таким чином зменшимо ризик проникнення в нашу мережу.

Хоча зловмисник може дізнатися *SSID* , проаналізувавши накопичений трафік, але наші дії все одно будуть певною перешкодою на його шляху. Тому в полі «*SSID Broadcast*» ми оберемо опцію «*Disabled*».

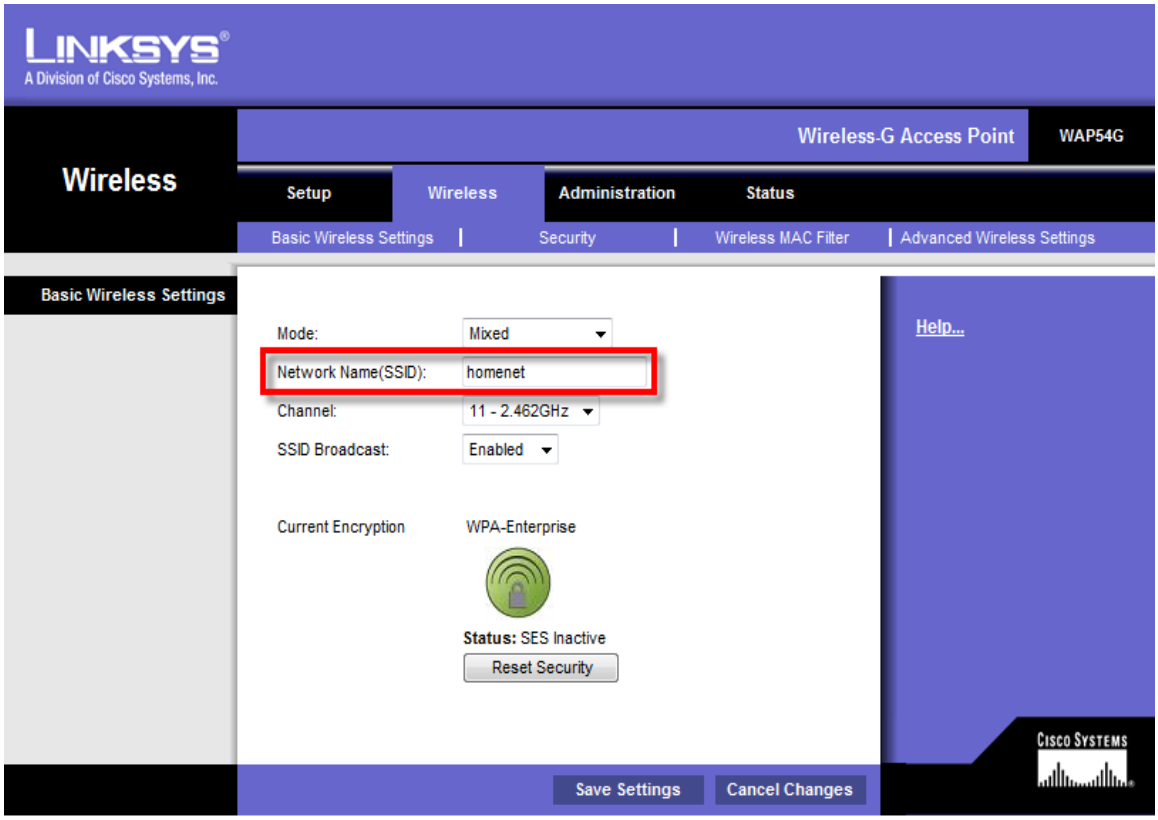

Рисунок 3.6 - Ім’я мережі

- засіб забезпечення безпеки *Wi-Fi* мережі - *WPA-Enterprise*.

Тут також вкажемо *IP* адресу *RADIUS*-сервера і секретний ключ, який ми вводили у вікні *Esomo APM* на вкладці «Точки доступа» розділу «*Wi-Fi*». У нас *IP* адреса *RADIUS*

- сервера – 192.168.0.1, а секретний ключ – *esomo*.

Натиснемо «*Save Settings*» для збереження налаштувань. З точкою доступу закінчено.

Налаштуємо наш комп'ютер для роботи в *Wi-Fi* мережі.

Перш за все встановимо створені та збережені цифрові сертифікати.

Для цього двічі клацнемо на сертифікаті лівою кнопкою миші та далі будемо слідувати інструкціям. На комп'ютері кожного користувача встановимо кореневий сертифікат та сертифікат даного користувача. Для сертифіката користувача необхідно буде ввести пароль.

Переглянути встановлені сертифікати ми можемо через браузер. Для цього оберемо «Сервіс» - «Властивості» - вкладка «Вміст» та натиснемо кнопку «Сертифікати». В розділі «Особисті» ми бачимо сертифікати користувачів (див. рис. 3.7), а в розділі «Довірені корневі центри сертифікації» - кореневий сертифікат.

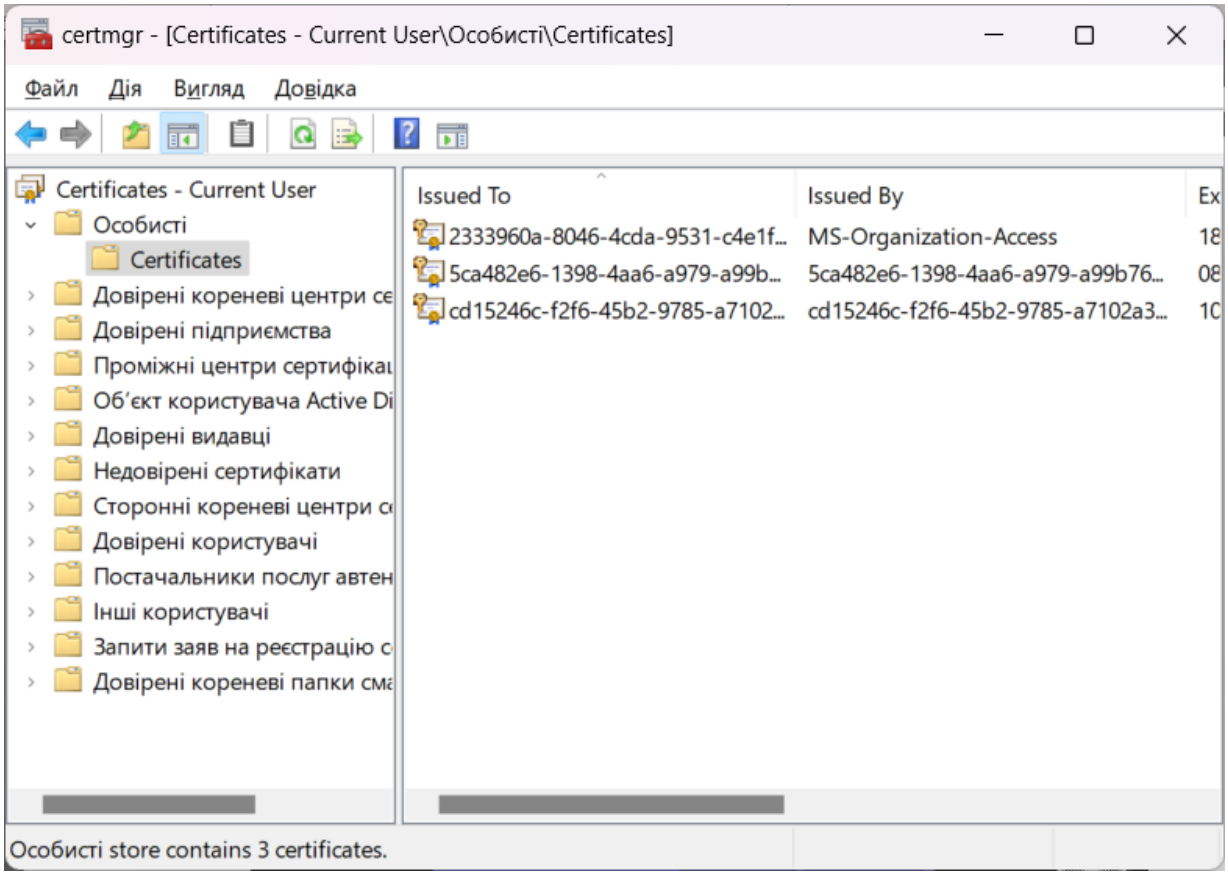

Рисунок 3.7 - Вікно встановлення сертифікату користувача

Підключитися до мережі *Wi-Fi* ми зможемо наступного дня, коли почнуть діяти сертифікати. Увімкнемо комп'ютер з *Esomo* та почекаємо кілька хвилин , поки бездротовий адаптер не знайде мережу. Вкажемо у властивостях мережі тип безпеки *WPA-Enterprise* та оберемо кореневий сертифікат для перевірки справжності. Налаштуємо *Wi-Fi* мережу для *Windows.*

З меню «Пуск» оберемо пункт «Підключення». Тут знайдете всі мережеві підключення, в тому числі і знайдена комп'ютером захищена бездротова мережа. Якщо ми клацнемо правою клавішею миші по її назві і оберемо пункт «Властивості», то відкриється вікно властивостей нашої бездротової мережі.

У полі «Тіп безпеки» оберіть «*WPA-Enterprise*», а в полі «Тіп шифрування» - «*AES*». У якості перевірки справності мережі беремо «*Microsoft*: Смарт-карта або інший сертифікат». Поставимо мітку навпроти пункту «Зберегти інформацію про користувачеві для післядуючого підключення до цієї мережі».

Натиснемо кнопку «Параметри». У вікні сертифіката влади встановлюємо позначки, а зі списку сертифікатів беремо кореневий сертифікат комп'ютера з *Esomo* (створений нами за допомогою *Esomo ARM* і встановлений на нашому комп'ютері). Натиснемо кнопку «ОК» у цьому та наступному вікні

Через кілька секунд ми можемо звернути нашу бездротову мережу та натиснути «Підключити».

3.3 Представлення застосованих алгоритмів для захисту *Wi-Fi* мережі

RADIUS – протокол призначений для співпраці з сервером аутентифікації, яким є *RADIUS* – сервер. Таким чином наша точка доступу налаштована для роботи в *Enterprise* – режимі.

Перевага використання серверу аутентифікації полягає в наданні можливості адміністратору забороняти доступ до мережі конкретним користувачам, а не їх комп'ютерам. Цей процес вимагає наявність окремих ключів шифрування для

кожного користувача. Системи аутентифікації, що підтримують динамічне створення ключів спрощують задачу адміністратора. При проходженні процедури аутентифікації ключі шифрування назначаються та анулюються автоматично, а для видалення будь-якого користувача із мережі достатньо видалити його обліковий запис.

Стандарт 802.1*x* заснований на принципах, характерних для протоколу типу «точка-точка» (*Point-to-Point Protoco, PPP*) і має назву розширений протокол аутентифікації (*Extensible Authentication Protocol, EAP*).

Аутентифікація по стандарту 802.1*x* вимагає наявності трьох складових:

Заявник – знаходиться на стороні клієнта мережі.

Аутентифікатор – знаходиться в точці доступу.

Сервер аутентифікації – розміщений на *RADIUS* – сервері.

Аутентифікатор створює логічний порт для пристрою заявника , що базується на ідентифікаторі асоціації (*AID*). Він організовує два шляхи для проходження трафіку – контрольований та неконтрольований.

Контрольований блокує весь трафік до тих пір, поки не буде успішно пройдена аутентифікація.

Алгоритм аутентифікації (див. рис. 3.8) повинен передбачати двосторонню аутентифікацію, динамічну генерацію ключів шифрування та аутентифікацію користувача.

1. Користувач – заявник для отримання доступу до середовища відправляє точці доступу повідомлення *EAP- Start,* інкапсульоване за стандартом 802.1*x.*

2. Точка доступу блокує клієнтський порт , дозволяючи передавати по мережі лише трафік стандарту 802.1*x.*

3. Точка доступу відправляє клієнту повідомлення з *EAP*- запитом на ідентифікацію (*EAP-Request Identity*).

4. Клієнт через *EAP*-відповідь (*EAP-Response*) повідомляє ім’я клієнта.

5. Точка доступу перенаправляє ім’я користувача до *RADIUS* – сервера для доступу (*RADIUS Access-Request*) на сервер аутентифікації .

6. *RADIUS* – сервер відправляє повідомлення з викликом (*Challenge Message*) в пакеті відповіді сервера *RADIUS* на прохання доступу (*RADIUS Access-Response*) клієнту, через точку доступу.

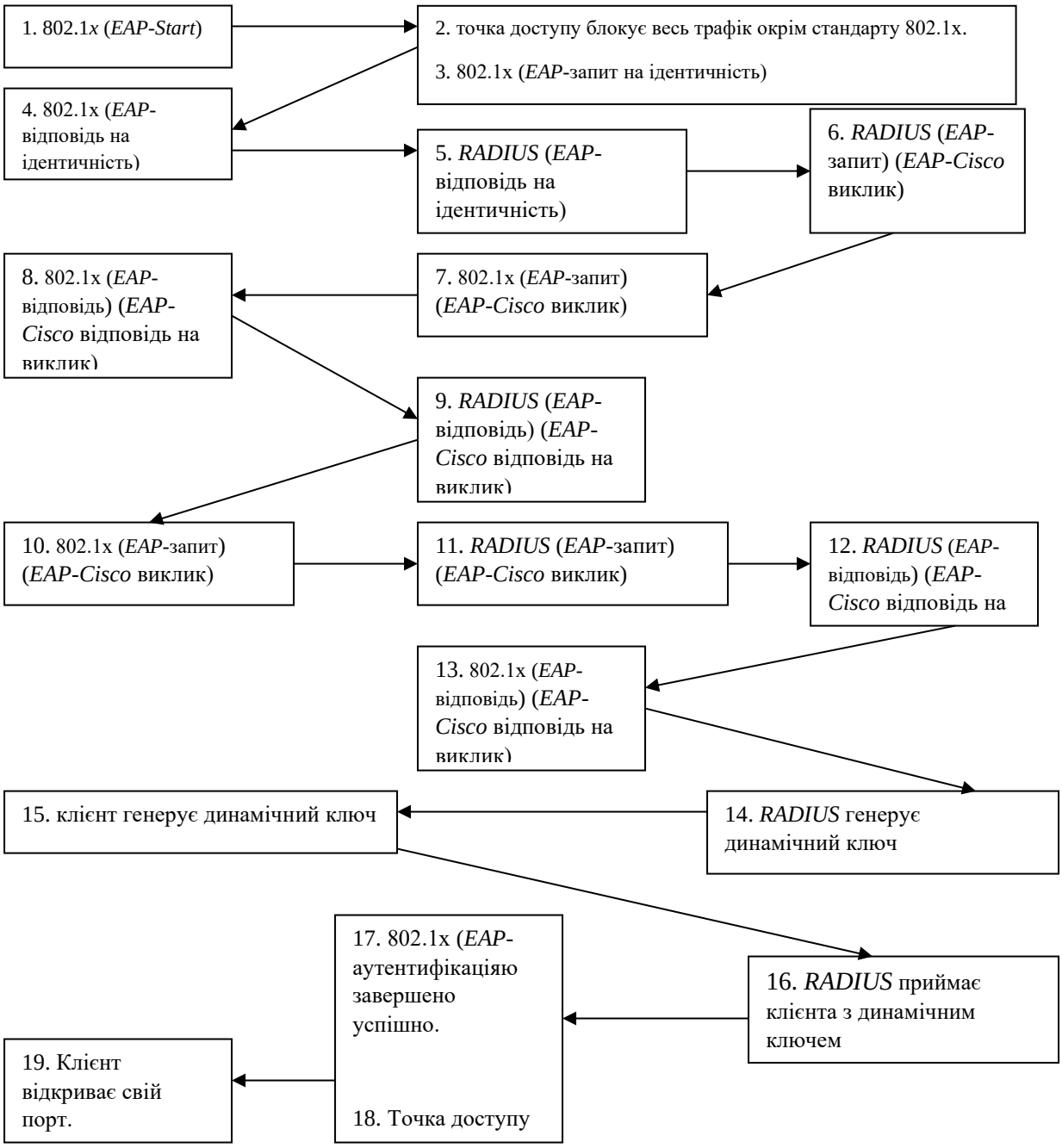

Рисунок 3.8 - Алгоритм аутентифікації

7. Точка доступу перенаправляє виклик клієнту.

8. Клієнт опрацьовує виклик та відправляє відповідь на *RADIUS* – сервер через точку доступу.

9. Точка доступу інкапсулює відповідь в пакет запиту до сервера *RADIUS* на доступ (*RADIUS Access-Request*) та перенаправляє її на сервер *RADIUS.*

10. Клієнт відправляє запит на сервер через точку доступу, щоб аутентифікувати мережу.

11. Точка доступу інкапсулює виклик в пакет відповіді серверу *RADIUS* на прохання доступу (*RADIUS Access-Response*).

12. Сервер *RADIUS* відправляє відповідь клієнту через точку доступу, інкапсульовану в пакет відповіді сервера *RADIUS* на прохання доступу (*RADIUS Access-Response*).

13. Точка доступу відправляє інкапсульовану відповідь клієнту.

14. Сервер *RADIUS* генерує динамічний ключ шифрування (*Dynamic Encryption Key*) на основі пароля користувача та сесійної інформації.

15. Клієнт генерує такий же ключ.

16. Сервер *RADIUS* відправляє свій ключ точці доступу, інкапсульований в пакет *RADIUS Accept*. Цей пакет вказує точці доступу на успішну аутентифікацію.

17. Точка доступу встановлює динамічний ключ для даного клієнта, інкапсулюючи повідомлення про успішну аутентифікацію – *EAP-Success.*

18. Точка доступу дозволяє перенаправлення трафіку через клієнтський порт .

19. Клієнт відкриває свій порт, при успішному завершенні взаємної аутентифікації.

Якщо користувачу необхідно заборонити доступ до мережі, то це можна реалізувати шляхом видалення його облікового запису.

ВИСНОВКИ

Виходячи з поставленої мети, а саме, спроектувати та налаштувати систему захисту *Wi-Fi* мережі, щоб уникнути несанкціонованого доступу та крадіжки інформації, ми прийшли до таких висновків та узагальнень:

1. Для порушників спосіб передачі інформації через радіоефір є найкращим, щоб перехопити, обробити та використати інформацію зі своєю метою. Радіоканал не забезпечує високого рівня захисту від прослуховування.

При здійсненні атака порушує головні властивості інформації, а саме її доступність, цілісність, конфіденційність. Найпоширеніші загрози: доступ до ресурсів і дисків користувачів *Wi-Fi*-мережі, а через неї і до ресурсів *LAN*, підслуховування трафіку, спотворення інформації, що проходить в мережі, користування інтернет-трафіком, атака ПК користувачів і серверів мережі, упровадження підроблених точок доступу, розповсюдження спаму.

2. Найефективнішим у побудові системи захисту бездротової мережі є поєднання засобів шифрування інформації та методів аутентифікації, як взаємної так і односторонньої.

3. Проаналізувавши існуючі методи ми розробили для нашої *Wi-Fi*-мережі таку систему захисту:

- організували перевірку справжності за цифровими сертифікатами за допомогою *RADIUS* сервера;

RADIUS сервера ми налаштували на основі програмного маршрутизатора *Esomo* з *FreeBSD* операційною системою на окремому комп’ютері. У роботі докладно описано його налаштування.

- забезпечили вихід в Інтернет через захищений канал з *VPN* шифруванням трафіку.

VPN канал формується автоматично при виході в Інтернет.

- заборонили широкомовну трансляцію *SSID* в ефір через налаштування точки доступу.

- змінили паролі для точки доступу та ім’я мережі.

- відключили опцію налаштування точки доступу через бездротовий інтерфейс.

- зменшили радіус випромінювання бездротової антени за межами офіса.

- всі наші клієнтські станції з’єднуються з точкою доступу, тому на них ми заборонили з’єднання в режимі *Ad-Hoc* , що унеможливить підключення зловмисника до однієї зі станцій. Для цього обрали тип мережі – *Infrastructure* в налаштуваннях мережевих карт.

- обмежили використання в бездротовій мережі протоколу *TCP/IP* для організації папок, файлів та принтерів загального доступу.

- обмежили гостьовий доступ до до загальних ресурсів.

- забезпечили використання довгих складних паролів та порекомендували зміну їх через два – три тижні.

- на всіх комп’ютерах в середині мережі встановили *FireWall* та антивірусне і антишпигунське програмне забезпечення. Це дасть нам змогу тримати в секреті персональні дані та уникнути викрадення паролів.

- порекомендували проводити своєчасне оновлення драйверів, прошивок, заплат для *Windows* , антивірусного та мережевого програмного забезпечення.

- порекомендували організацію регулярних перевірок стійкості засобів безпеки за допомогою спеціалізованих сканерів безпеки, наприклад *NetStumbler*.

Ці засоби здатні забезпечити достатньо високий рівень захисту у поєднанні з правильним адмініструванням мережі.

Були виконані всі поставлені задачі і спроектована надійна система захисту.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *ISO*/*IEC* 27001:2022. *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*. – Женева : *ISO,* 2022. – 50 с.

2. *NIST SP* 800-63*B Digital Identity Guidelines*: *Authentication and Lifecycle Management*. – Гейтерсберг : *NIST,* 2020. – 90 с.

3. *ISO*/*IEC* 29100:2011. *Information technology – Security techniques – Privacy framework*. – Женева : *ISO,* 2011. – 32 с.

4. *ISO*/*IEC* 11770-1:2010. *Information technology – Security techniques – Key management – Part* 1: *Framework*. – Женева : *ISO,* 2010. – 32 с.

5. *IEEE Std* 1363-2000. *Standard Specifications for Public Key Cryptography*. – Нью-Йорк : *IEEE,* 2000. – 178 с.

6. *OWASP Authentication Cheat Sheet*. – [Електронний ресурс]. – Режим доступу: *https*://*cheatsheetseries*.*owasp*.*org* (дата звернення: 06.06.2025).

7. *Microsoft Identity Platform*: *Authentication and Authorization Basics*. – [Електронний ресурс]. – Режим доступу: *https*://*learn*.*microsoft*.*com* (дата звернення: 06.06.2025).

8. *Cisco Zero Trust*: *Identity and Access Management*. – [Електронний ресурс]. – Режим доступу: *https*://*www*.*cisco*.*com* (дата звернення: 06.06.2025).

9. *RSA Encryption Algorithm* – [Електронний ресурс]. – Режим доступу: *https*://*www*.*rsa*.*com* (дата звернення: 06.06.2025).

10. *OpenID Foundation*. *OpenID Connect Core* 1.0. – [Електронний ресурс]. – Режим доступу: *https*://*openid*.*net*/*specs*/*openid-connect-core*-1_0.*html* (дата звернення: 06.06.2025).

11. Теслюк В.М., Базильчук Я.Ю. Бездротові інформаційні технології. – Львів : Видавництво Львівської політехніки, 2019. – 312 с.

12. Копець С.В. Основи інформаційної безпеки в мережах. – К. : Ліра-К, 2021. – 248 с.

13. Савченко О.Ф. Методи криптографічного захисту даних. – К. : Видавництво НАУ, 2020. – 204 с.

14. Андрієнко М.С. Технології автентифікації користувачів у комп’ютерних системах. – Харків : ХНУРЕ, 2021. – 192 с.

15. Теліженко М.М. Комп’ютерні мережі. Навчальний посібник. – Київ : Каравела, 2021. – 288 с.

16. Білоус О.В. Методи двофакторної автентифікації: аналіз і застосування. – Вісник ХНУРЕ. – 2023. – №2. – С. 51–59.

17. Захист інформації в інформаційних системах / за ред. І.О. Марченка. – Харків : ХНУРЕ, 2022. – 276 с.

18. Паламарчук В.С. Сучасні криптографічні протоколи: структура, реалізація, ефективність. – Вісник НТУУ «КПІ». Серія: Інформатика, управління та обчислювальна техніка. – 2023. – №1. – С. 45–53.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

РЕЦЕНЗІЯ
на кваліфікаційну роботу

випускника спеціальності: 123 «Комп'ютерна інженерія»

відділення: комп'ютерної та програмної інженерії

циклова комісія: комп'ютерних систем та мереж

Данило БАЛАЦЬКИЙ
(ім'я, прізвище)

1. Актуальність теми: Обрана тема кваліфікаційної роботи «Дослідження інтеграції засобів шифрування даних та методів авторизації користувачів» є актуальною.

2. Кваліфікаційна робота відповідає темі, затвердженій наказом.

3. Завдання на виконання кваліфікаційної роботи виконано у повному обсязі.

4. В результаті виконання кваліфікаційної роботи було встановлено, що, поєднання сучасних алгоритмів шифрування даних та авторизації користувачів за допомогою RADIUS-сервера дає максимальний захист мережі. Легке додавання користувачів дає можливість налаштувати гнучку мережеву структуру. Захищена мережа дасть змогу зберегти конфіденційність, цілісність та автентичність інформації та уникнути збитків від зламу мережі.

5. Якість виконання пояснювальної записки та ілюстративного (графічного) матеріалу відповідає вимогам Державних стандартів.

6. В кваліфікаційній роботі зроблений акцент на дані отримані на практиці («живі» експерименти).

7. Кваліфікаційна робота заслуговує оцінку «добре».

Рецензент ~~Доктор технічних наук, професор~~
(науковий ступінь, посада)

«____»_____ 2025 р. _____ Володимир АНДРУСЕВИЧ
(підпис) (ім'я, прізвище)

З рецензією ознайомлений _____ Данило БАЛАЦЬКИЙ
(підпис) (ім'я, прізвище)

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

ВІДГУК
керівника кваліфікаційної роботи

випускника спеціальності: 123 «Комп'ютерна інженерія»

відділення: комп'ютерної та програмної інженерії

циклова комісія: комп'ютерних систем та мереж

Данило БАЛАЦЬКИЙ
(ім'я, прізвище)

1. *Кваліфікаційна робота на тему «Дослідження інтеграції засобів шифрування даних та методів авторизації користувачів» виконана в ініціативному порядку.*
2. *Метою кваліфікаційної роботи є проектування та налаштування системи захисту мережі Wi-Fi, що дозволить запобігти несанкціонованому доступу до мережі та крадіжці корпоративної інформації.*
3. *Кваліфікаційна робота відповідає темі, затвердженій наказом начальника коледжу.*
4. *Кваліфікаційна робота виконана здобувачем освіти самостійно.*
5. *Здобувач освіти показав високі вміння роботи з літературними джерелами, аналіз теоретичного та практичного матеріалу, приймання обґрунтованих рішень, застосовування сучасних комп'ютерних інформаційних технологій.*
6. *Данило БАЛАЦЬКИЙ показав достатній рівень дотримання вимог державних стандартів при виконанні кваліфікаційної роботи в цілому та оформленні пояснювальної записки.*
7. *Рівень виконаної кваліфікаційної роботи заслуговує оцінку «добре», відповідає набутих випускником знань, умінь та навичок, вимогам освітньої характеристики фахівця і можливість присвоєння йому кваліфікації фахівця освітнього ступеня «бакалавр» спеціальності 123 «Комп'ютерна інженерія».*

Керівник кваліфікаційної роботи

«06» 06 2025 р. _____ Галина ДАНИЛІНА
(підпис) (ім'я, прізвище)