МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»
Галузь знань 12 «Інформаційна безпека»
Спеціальність 125 «Кібербезпека»

Форма навчання: очна(денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему «Забезпечення інформаційної безпеки у корпоративній локальній мережі на основі технології Wi-Fi»

здобувача Кулаковської Аліни Сергіївни _____
(підпис)

Науковий керівник: к.т.н., доц. Корольов А.П.

_____
(підпис)

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: д.ф.м.н., проф. Джалладова І.А.

_____
(підпис)

Київ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»
Галузь знань 12 «Інформаційна безпека»
Спеціальність 125 «Кібербезпека»

ПОГОДЖЕНО	**ЗАТВЕРДЖУЮ:**
Керівник проектної групи (гарант) освітньо-професійної програми	Завідувач кафедри
Мамонова Г. В.	Джалладова І.А.
(підпис) (ініціали,призвище)	*(підпис) (ініціали,призвище)*
_____ 20__р.	_____ 20__р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти Кулаковської Аліни Сергіївни
(прізвище, ім'я, по батькові)
очної(денної) **форми навчання**
очної (денної), заочної, дистанційної

на підготовку кваліфікаційної бакалаврської роботи

на тему «Забезпечення інформаційної безпеки у корпоративній локальній мережі на основі технології Wi-Fi »

Тему затверджено наказом ректора Університету від «___»_____20__р.№___

Кваліфікаційна бакалаврська робота виконується на матеріалах

_____

_____

План кваліфікаційної бакалаврської роботи

Розділ 1 | Аналіз стану розвитку та проблеми інформаційної безпеки в області безпроводових локальних мереж на основі технології Wi-Fi

Розділ 2 | Планування та розгортання мережі на базі технології Wi-Fi

Розділ 3 | Забезпечення інформаційної безпеки мережі Wi-Fi

Об'єкт дослідження: | корпоративна локальна мережа на основі технології Wi-Fi.

Предмет дослідження: | методи та засоби забезпечення інформаційної безпеки в корпоративній локальній мережі, яка використовує технологію Wi-Fi.

Мета кваліфікаційної бакалаврської роботи: | розробка та впровадження стратегій і заходів забезпечення інформаційної безпеки в корпоративних локальних мережах на основі технології Wi-Fi для запобігання потенційним загрозам і збереження конфіденційності даних.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1 | провести огляд сучасного стану технології Wi-Fi, включаючи останні версії стандартів та їхні особливості; проаналізувати основні вразливості та загрози інформаційної безпеки, що характерні для безпроводових мереж; оцінити поточні методи та засоби захисту інформації у Wi-Fi мережах

У розділі 2 | розробити структурну схему Wi-Fi мережі; обґрунтувати та вибрати оптимальне обладнання; розрахувати зони покриття Wi-Fi обладнання; виконати розрахунок IP-адрес та планування каналів для забезпечення належної роботи мережі без конфліктів та з максимальною пропускною здатністю

У розділі 3 | розробити та впровадити комплексні системи захисту інформації під час розгортання Wi-Fi мережі; налаштувати безпечну роботу пристроїв корпоративної бездротової мережі; розробити політику інформаційної безпеки, яка регламентує використання та захист даних у корпоративній бездротовій мережі.

Завдання підготував
науковий керівник

_____ Корольов А.П.
(підпис) (прізвище, ініціали)

Завдання одержав
здобувач _____ Кулаковська А.С.
(підпис) (прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна бакалаврська робота: 71 С., 9 РИС., 6 ТАБЛ., 28 ДЖЕРЕЛ.

Об’єкт дослідження: корпоративні локальні мережі з використанням технології Wi-Fi.

Мета кваліфікаційної роботи: розробка та впровадження стратегій і заходів забезпечення інформаційної безпеки в корпоративних локальних мережах на основі технології Wi-Fi для запобігання потенційним загрозам і збереження конфіденційності даних.

Методи дослідження: аналітичний огляд існуючих методів кіберзахисту корпоративного середовища, порівняльний аналіз технологій для побудови захищеної корпоративної мережі, імітаційне моделювання з використанням програмного забезпечення Cisco Packet Tracer (при розробці схеми мережі), експериментальні дослідження (налаштування роутера).

Практичне значення роботи полягає у розробці та впровадженні ефективних заходів забезпечення інформаційної безпеки для корпоративної локальної мережі на основі технології Wi-Fi, що дозволить уникнути потенційних загроз та зберегти конфіденційність даних.

Результати здійснених у кваліфікаційній роботі досліджень можуть бути використані для розробки та впровадження заходів забезпечення інформаційної безпеки в корпоративних локальних мережах на основі технології Wi-Fi, що сприятиме зменшенню ризиків порушення безпеки та захисту конфіденційної інформації.

Наукова новизна дослідження полягає у тому, що воно пропонує інтегрований підхід до забезпечення інформаційної безпеки у корпоративних локальних мережах основі технології Wi-Fi, що враховує сучасні загрози та ризики, та розробляє практичні рекомендації для їх ефективного запобігання.

Напрямки подальших досліджень: розробка більш ефективних методів виявлення та усунення потенційних безпекових проблем у бездротових мережах Wi-Fi; аналіз впливу нових технологій та стандартів безпеки на стійкість корпоративних мереж до атак; вдосконалення методів управління безпекою мережі для забезпечення відповідності стандартам та регулятивним вимогам.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЇ, БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ, ТЕХНОЛОГІЯ WI-FI, ШИФРУВАННЯ WI-FI, ЗАГРОЗИ В БЕЗДРОТОВІЙ МЕРЕЖІ.

ВІДГУК

на кваліфікаційну бакалаврську роботу

студента Кулаковської Аліни Сергіївни гр. ІК-401

на тему: Забезпечення інформаційної безпеки у корпоративній локальній мережі на основі технології Wi-Fi

Актуальність теми. На сьогоднішній день локальні мережі на основі технології Wi-Fi широко використовуються в корпоративних інформаційних системах. Але з усіх бездротових мереж вони найбільш вразливі з точки зору інформаційної безпеки. Тому тема роботи є актуальною.

Повнота розкриття теми. Поставлені в роботі задачі вирішені в повному обсязі. Тема розкрита на достатньому рівні.

Теоретичний рівень представленого матеріалу та отриманих результатів високий, відповідає вимогам до кваліфікаційних бакалаврських робіт.

Практична значущість роботи полягає в тому, що розроблений комплекс заходів з забезпечення інформаційної безпеки може бути використаний при плануванні та розгортанні реальних Wi-Fi мереж.

Самостійність виконання роботи. Робота виконана здобувачем повністю самостійно.

Якість оформлення, загальна та спеціальна грамотність. Є окремі помилки з граматики та стилістики викладення текстового матеріалу. В цілому якість оформлення відповідає діючим вимогам.

Переваги та недоліки роботи. Перевагою роботи є використання імітаційного моделювання шляхом використання багатофункціональної програми моделювання мереж *Cisco Packet Tracer при розробці та моделювання схеми мережі. До недоліків можна віднести слабкий аналіз перспектив розвитку* Wi-Fi мереж та систем їх захисту.

Загальна оцінка роботи та висновок щодо рекомендації до захисту в ЕК.
В цілому бакалаврська робота здобувача Кулаковської А.С. відповідає вимогам щодо кваліфікаційних робіт бакалаврів за спеціальністю 125 Кібербезпека і заслуговує оцінки «добре», рекомендується для захисту в ЕК.

Науковий керівник

Професор кафедри системного аналізу
та кібербезпеки _____ А.П. Корольов

“____”_____2024 р.

РЕЦЕНЗІЯ
на кваліфікаційну бакалаврську роботу

студента Кулаковської А.С. гр. ІК-401

на тему: Забезпечення інформаційної безпеки у корпоративній локальній мережі на основі технології Wi-Fi

Актуальність теми обумовлена широкою популярністю мереж Wi-Fi. Переваги бездротових Wi-Fi мереж вагомі: швидке розгортання; відсутність проводів; достатньо висока швидкість і т. інш. Але є і недоліки, пов'язані наприклад з забезпеченням безпеки мереж Wi-Fi. Особливо це актуально для корпоративних мереж. Тому тема роботи є актуальною.

Наукова новизна полягає в тому, що крім традиційних заходів забезпечення інформаційної безпеки розглянуті сучасні загрози та ризики, розроблені практичні рекомендації для їх ефективного запобігання.

Якість проведеного аналізу. В першому розділі проведений аналіз стану розвитку та проблеми інформаційної безпеки в області безпроводових локальних мереж на основі технології Wi-Fi. Наведений в роботі матеріал свідчить про достатньо високу якість проведеного аналізу.

Уміння користуватися літературними джерелами. Наведений перелік свідчить про уміння здобувача користуватись літературними джерелами. Перелік включає сучасні джерела інформації як українських, так і провідних зарубіжних видань. Широко використані матеріали, що є в електронному доступі в Інтернеті.

Практична цінність висновків і рекомендацій. Вони можуть бути використані при плануванні та розгортанні реальних корпоративних локальних мереж на основі технології Wi-Fi для забезпечення їх інформаційної безпеки.

Переваги та недоліки. Перевагами роботи є її комплексний характер, спрямований на вирішення в цілому задачі розгортання корпоративної локальної мережі на основі технології Wi-Fi. При цьому особлива увага приділяється інформаційній безпеці, що відповідає спеціальності здобувача. До недоліків можна віднести відсутність розгляду перспектив вдосконалення методів управління безпекою мережі.

Загальний висновок і оцінка роботи. В цілому бакалаврська робота здобувача Кулаковської А.С. відповідає вимогам щодо кваліфікаційних робіт бакалаврів і заслуговує оцінки «добре», а автор присвоєння кваліфікації бакалавр за заявленою спеціальністю 125 Кібербезпека.

Рецензент
Доцент кафедри телекомунікаційних мереж та систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут

_____ М.Д. Ільїнов

"___"_____2024р.

ЗМІСТ

ВСТУП

Технологія Wi-Fi є однією з найпоширеніших технологій бездротового доступу до мережі Інтернет. Вона використовується в корпоративних локальних мережах для забезпечення доступу до ресурсів мережі для співробітників, а також для надання послуг клієнтам. Мережа Wi-Fi має низку переваг перед традиційними проводовими мережами. Вони більш мобільні, прості в установці та експлуатації, а також дозволяють економити на витратах на кабельну інфраструктуру. Однак, разом з тим, Wi-Fi-мережі є більш вразливими до атак, ніж проводові мережі. Це пов'язано з тим, що сигнал Wi-Fi може бути перехоплений із значної відстані. У сучасних організаціях все більше даних зберігається та обробляється в локальних мережах. Це робить ці мережі більш привабливими для атак зловмисників. Зловмисники постійно розробляють нові методи атак на інформаційну безпеку, включаючи корпоративні мережі Wi-Fi, що вимагає від організацій удосконалення заходів безпеки корпоративні мережі Wi-Fi.

Значний вклад в розвиток Wi-Fi технологій в Україні внесли О. В. Іванов, І. Прокопович, В. Маланюк, В. Попель, В. Шкурко, В. Галайчук, В. Слободянюк та інші. Серед закордонних науковців варто згадати V. Hayes, B. Tuch, C. Links, R. McGinn та інших.

У результаті проведених досліджень було вирішено ряд задач у сфері забезпечення інформаційної безпеки у корпоративній локальній мережі на основі технології Wi-Fi. Зокрема, були розроблені ефективні методи та засоби захисту від таких загроз, як фізичний доступ до точки доступу, радіоперехоплення та атаки на шифрування. Однак, у цій сфері існують і ряд проблем, які потребують подальшого дослідження. Серед таких проблем можна виділити такі: зростання складності та витонченості кібератак; недостатня обізнаність працівників про інформаційну безпеку, що призводить до неправильного використання корпоративної локальної Wi-Fi мережі.

Результати досліджень у рамках даної тематики можуть бути використані для підвищення рівня інформаційної безпеки корпоративних локальних мереж, що використовують Wi-Fi. Тому, дослідження в галузі забезпечення інформаційної безпеки у Wi-Fi-мережах є актуальним та перспективним напрямком.

Мета роботи полягає в розробці та впровадженні стратегій і заходів забезпечення інформаційної безпеки в корпоративних локальних мережах на основі технології Wi-Fi для запобігання потенційним загрозам і збереження конфіденційності даних.

Для досягнення зазначеної мети кваліфікаційної роботи поставлені окремі завдання:

- провести аналізі існуючих методів та засобів забезпечення безпеки корпоративних локальних мережах Wi-Fi;
- вивченні сучасного стану проблеми забезпечення інформаційної безпеки у корпоративних локальних мережах на основі технології Wi-Fi;
- впровадження і налаштування відповідних технічних засобів і програмного забезпечення для забезпечення безпеки Wi-Fi мережі;
- розробка плану та рекомендацій забезпечення інформаційної безпеки у корпоративних локальних мережах;

Об'єкт дослідження - корпоративні локальні мережі на основі технології Wi-Fi.

Предмет дослідження - методи та засоби забезпечення інформаційної безпеки у Wi-Fi мережах.

У дослідженні будуть використані такі методи дослідження:

- аналіз наукової літератури та нормативно-правової бази;
- аналіз існуючих методів та засобів забезпечення інформаційної безпеки;
- імітаційне моделювання та експериментальні дослідження.

Теоретична і методична значущість отриманих результатів:

- розроблені методи та засоби підвищення рівня безпеки корпоративних локальних мереж на основі технології Wi-Fi;

- вивчено основні загрози та вразливості корпоративних локальних мереж на основі технології Wi-Fi;
- використання методів моделювання та експериментальних досліджень дозволило отримати об'єктивні результати дослідження.

Практична цінність роботи полягає в наступному:

- підвищення рівня безпеки корпоративних локальних мереж на основі технології Wi-Fi;
- отримані результати дослідження можуть бути використані для розробки нових методів та засобів захисту таких мереж, які будуть більш ефективними та здатними протистояти сучасним кібератакам.

РОЗДІЛ 1. АНАЛІЗ МОЖЛИВОСТЕЙ ТЕХНОЛОГІЇ БЕЗДРОТОВОГО ЗВ'ЯЗКУ WI-FI ДЛЯ ПОБУДОВИ КОРПОРАТИВНИХ ЛОКАЛЬНИХ МЕРЕЖ

Забезпечення інформаційної безпеки у корпоративній локальній мережі на основі технології Wi-Fi є критично важливим з огляду на зростання загроз та ризиків, пов'язаних з кібербезпекою. Корпорації залежать від безперебійного та безпечного функціонування своїх мереж для забезпечення комунікації, обміну даними та виконання бізнес-процесів. В умовах розширення роботи на віддалених місцях, зростання кількості мобільних пристроїв та обсягів обміну даними, безпека Wi-Fi мереж стає ще більш критичною. Ефективне захист мережі Wi-Fi дозволяє уникнути потенційних загроз, таких як несанкціонований доступ до конфіденційної інформації, зловживання мережевими ресурсами та розповсюдження шкідливих програм, що може призвести до фінансових втрат, порушень репутації та інших серйозних наслідків для підприємства. Таким чином, інвестування в надійність та безпеку корпоративних Wi-Fi мереж є вирішальною складовою стратегії управління ризиками та забезпечення стійкості діяльності організації. Тому питання інформаційної безпеки завжди мають велике значення в розвитку будь-якого підприємства.

Інформаційну безпеку можна охарактеризувати як процес забезпечення конфіденційності, цілісності, доступності та спостереженості інформації, що зберігається, передається або обробляється в інформаційних системах. Цей процес включає в себе застосування технічних, організаційних та процедурних заходів для захисту інформації від несанкціонованого доступу, модифікації або втрати, а також забезпечення її належної доступності для авторизованих користувачів відповідно до їхніх прав та привілеїв.

Бездротова технологія Wi-Fi стала неодмінною складовою сучасних корпоративних інфраструктур, забезпечуючи ефективну комунікацію та зручний доступ до мережних ресурсів. Цей розділ присвячений детальному аналізу можливостей цієї технології з врахуванням ключових аспектів, таких як принципи

роботи, стандарти мереж Wi-Fi, архітектура та обладнання мережі. Додатково, вивчається аспект інформаційної безпеки бездротових мереж зв'язку, проводиться аналіз існуючих проблем та висвітлюються підходи до їхнього вирішення.

1.1 Постановка задачі

Необхідно виконати планування та необхідні розрахунки для організації захищеної корпоративної локальної мережі Wi-Fi з виконанням наступних умов:

– мережа охоплює 1-й та 2-й поверхи будівлі;

– на 1-му поверсі забезпечено дротове підключення мережі Internet;

– матеріал перекриття між поверхами – залізобетонні плити;

– матеріал зовнішніх стін та внутрішніх стін будівлі – газоблоки;

– на 1-му поверсі розташовані 10 робочих місць користувачів, які мають 4 ПК, 6 ноутбуків та принтер з Wi-Fi адаптерами;

– на 2-му поверсі розташовані 4 робочих місця користувачів з 1ПК, 3 ноутбуками, принтером з Wi-Fi адаптерами;

– відстань між користувачами на одному поверсі не перевищує 50 метрів;

– IP-адреса мережі 192.168.255.0 і мережева маска для неї 255.255.255.0;

– створити дві підмережі за кількістю поверхів і розробити IP-адреси для користувачів;

– забезпечити інформаційну безпеку розробленої мережі.

1.2 Поняття та принцип роботи Wi-Fi

Wi-Fi - це сімейство бездротових мережевих протоколів, заснованих на сімействі стандартів IEEE 802.11, які зазвичай використовуються для локального об'єднання пристроїв і доступу до Інтернету, дозволяючи розташованим поблизу цифровим пристроям обмінюватися даними за допомогою радіохвиль [1, с.6]. Wi-Fi працює в неліцензованому ISM-спектрі, його легко розгорнути будь-кому і будь-де, а необхідне обладнання є простим і дешевим.

У мережах Wi-Fi немає фізичного дротового з'єднання між передавачем і приймачем. Натомість вони працюють із використанням радіочастотної технології - частот електромагнітного спектра, пов'язаних із поширенням радіохвиль: під час подачі радіочастотного струму на антену генерується електромагнітне поле, що поширюється в просторі.

Основою бездротової мережі є точка доступу. ЇЇ головна роль полягає в передачі бездротового сигналу, який комп'ютер може використовувати для виявлення та встановлення мережевого з'єднання [1, с.16]. Щоб під'єднатися до бездротової мережі, комп'ютер або іший пристрій мають бути оснащені адаптером бездротової мережі.

Принцип роботи Wi-Fi полягає у встановленні бездротового з'єднання між пристроями за допомогою радіосигналів. Wi-Fi покладається на уникнення колізій (CSMA/CA), де кожен відправник намагається уникнути колізій, передаючи лише тоді, коли канал не зайнятий, а потім надсилає свій повний кадр повідомлення повністю [2, с.531]. Після відправлення кадру Wi-Fi відправник чекає на підтвердження від одержувача, перш ніж приступити до наступної передачі. Процес можна розділити на кілька кроків, які наведені нижче:

1. Створення мережі. Пристрої, які підтримують Wi-Fi, можуть діяти як точки доступу (наприклад, маршрутизатори або смартфони з функцією гарячої точки), які створюють бездротову мережу, до якої можуть підключатися інші пристрої.

2. Пошук доступних мереж. Пристрої, які шукають Wi-Fi, сканують оточуючі радіочастоти, щоб знайти доступні мережі Wi-Fi.

3. Аутентифікація і авторизація. Коли пристрій знаходить мережу, він може спробувати підключитися до неї. Цей процес включає в себе аутентифікацію (перевірку правильності пароля або іншої ідентифікаційної інформації) і авторизацію (отримання підтвердження від точки доступу про успішне підключення).

4. Передача даних. Після успішного підключення пристрої можуть обмінюватися даними через бездротове з'єднання. Маршрутизатор відправляє інформацію в Інтернет за допомогою фізичного дротового з'єднання Ethernet.

5. Завершення з'єднання. Коли пристрої більше не потрібно підключення, вони можуть розірвати з'єднання.

Усі електронні пристрої зчитують дані в двійковому форматі, як і маршрутизатори так і інші пристрої. Роутер випромінює радіохвилі, які приймають наші пристрої, і зчитує їх у двійковому вигляді. Де верхній пік радіохвилі відповідає "1", а нижній - "0".

Кожна мережа Wi-Fi має свій ідентифікатор, що відомий як SSID (Service Set Identifier). Цей ідентифікатор визначає мережу та дозволяє пристроям знаходити і підключатися до неї. Також, як і в інших локальних мережах IEEE 802, кожна Wi-Fi станція має унікальну адресу, оскільки вони програмуються з глобально унікальними 48-бітовими MAC-адресами. MAC-адрес використовується для ідентифікації як пункту призначення, так і джерела кожного пакета даних. Wi-Fi встановлює з'єднання на канальному рівні і може бути ідентифікований як за адресою призначення, так і за адресою джерела. Коли приймач отримує передачу, він використовує адресу призначення, щоб визначити, чи важлива ця передача для станції, чи її слід проігнорувати.

Переваги технології Wi-Fi.

1. Бездротовий доступ до Інтернету. Wi-Fi дозволяє користувачам підключатися до Інтернету без потреби в проводових з'єднаннях, що забезпечує високий рівень мобільності.

2. Зручність і легкість встановлення. Встановлення Wi-Fi мережі зазвичай досить просте і не вимагає прокладання дротів по всьому приміщенню.

3. Широке покриття. Wi-Fi може забезпечити покриття великих приміщень, офісів, громадських місць і навіть відкритих територій, якщо він належним чином налаштований.

4. Зв'язок з багатьма пристроями. Wi-Fi може обслуговувати одночасно багато пристроїв, що робить його ідеальним рішенням для домашнього використання, офісів та громадських місць.

Недоліки технології Wi-Fi.

1. Обмежена швидкість. Швидкість передачі даних через Wi-Fi може бути обмеженою, особливо при великій кількості підключених пристроїв або в умовах перешкод, таких як стіни або інші перешкоди.

2. Потенційна небезпека. Бездротові мережі, включаючи Wi-Fi, можуть бути підвернуті ризику хакерських атак і несанкціонованого доступу до даних, якщо не застосовуються відповідні заходи безпеки.

3. Обмеження дальності сигналу. Сигнал Wi-Fi може бути обмежений в дальність, особливо в умовах перешкод, що може призвести до втрати зв'язку або зниження швидкості.

1.3 Стандарти мереж Wi-Fi

Стандарти Wi-Fi - це набори технічних специфікацій, які визначають основні характеристики бездротових мереж. Wi-Fi технологія базується на стандартах IEEE 802.11 - набір технічних стандартів локальних обчислювальних мереж (LAN) і визначає набір протоколів керування доступом до середовища (MAC) і фізичного рівня (PHY) для реалізації бездротового зв'язку комп'ютерів у локальних обчислювальних мережах (WLAN) [3, с.11].

Кожен стандарт мережі Wi-Fi має два параметри :

- швидкість передачі даних у мережі;
- частота на якій радіочастоті працює мережа.

На частоті 2,4 ГГц дані передаються повільніше, ніж на частоті 5 ГГц, але мають більший радіус дії, ніж на частоті 5 ГГц. На частоті 5 ГГц дані передаються швидше, але радіус дії менший, оскільки вона має вищу частоту.

Таблиця 1.1 – Покоління стандартів Wi-Fi

Стандарт	Частотний діапазон	Швидкість передачі	Особливість
802.11a	5 ГГц	до 54 Мбіт/с	Обмежена сумісність з іншими стандартами через використання високочастотного діапазону
802.11b	2,4 ГГц	до 11 Мбіт/с	Сумісність з широким спектром пристроїв, але підвищена вразливість до перешкод
802.11g	2,4 ГГц	до 54 Мбіт/с	Зворотна сумісність з 802.11b, але схильний до перешкод від інших пристроїв у тому ж діапазоні
802.11n	2,4 ГГц та 5 ГГц	до 600 Мбіт/с	Використання технології MIMO (Multiple Input, Multiple Output) для підвищення пропускної здатності та покращення стабільності з'єднання
802.11ac	5 ГГц	до 1,3 Гбіт/с	Підтримка широкосмугових каналів (80 МГц і 160 МГц) для підвищення продуктивності
802.11ax (Wi-Fi 6)	2,4 ГГц та 5 ГГц (з можливістю розширення до 6 ГГц у Wi-Fi 6E)	до 9,6 Гбіт/с	Використання технології OFDMA (Orthogonal Frequency Division Multiple Access) для ефективнішого використання спектру і зменшення затримок Підвищена енергоефективність та продуктивність в умовах високої щільності підключень

Джерело: розроблено автором на основі [4]

Різні версії Wi-Fi базуються на різних стандартах протоколу IEEE 802.11, і кожна з них визначає використовуваний радіодіапазон, максимальну дальність та швидкість передачі даних. Wi-Fi зазвичай працює у радіодіапазонах, які поділяються на кілька каналів: три канали для 2,4 ГГц і чотирнадцять для 5 ГГц. У мережі можуть існувати спільні канали, проте лише один передавач може одночасно використовувати кожен канал у межах конкретного діапазону.

802.1X - це стандарт, який використовується для безпечної бездротової автентифікації користувачів та/або пристроїв, а також для обміну ключами [5, с.35]. 802.1X прописується, коли налаштовується SSID з "корпоративним" рівнем безпеки, а саме WPA2-Enterprise і WPA3-Enterprise. Захищені корпоративні мережі використовують IEEE 802.1X з EAP для автентифікації та обміну ключами. Це золотий стандарт для автентифікації користувачів і пристроїв у бездротовій мережі, який може включати в себе імена-паролі, токени, сертифікати або їх комбінації для багатофакторної автентифікації (MFA). 802.1X вимагає, щоб бездротова інфраструктура і кінцеві точки підтримували протокол 802.1X і мали певні можливості автентифікації - як сервери, так і кінцеві точки - один з одним. Він також вимагає наявності належним чином налаштованого сервера автентифікації (зокрема сервера RADIUS).

RADIUS (Remote Authentication Dial-In User Service) - це широко використовуваний мережевий протокол, який забезпечує централізовану автентифікацію, авторизацію та облік (AAA) для користувачів, які отримують доступ до віддаленої мережі за допомогою протоколу UDP [6, с.15]. Він забезпечує безпечний та ефективний спосіб керування контролем доступу та автентифікацією користувачів, дозволяючи мережевим адміністраторам контролювати доступ користувачів до ресурсів на основі політик та дозволів. RADIUS це клієнт-серверний протокол що працює на прикладному рівні, і може використовувати як протокол трансортування TCP так і UDP.

Стандарти мереж Wi-Fi є важливими для розробки, розгортання та ефективної експлуатації бездротових мереж. Вони визначають технічні характеристики, протоколи безпеки та методи комунікації між пристроями. З розвитком технологій безпеки, таких як WPA3, а також з вдосконаленням швидкості та дальності зв'язку у нових версіях стандартів, мережі Wi-Fi стають все надійнішими та зручнішими для використання у різних сферах життя. Ці стандарти постійно оновлюються та вдосконалюються, щоб відповідати зростаючим вимогам користувачів у швидкості, безпеці та доступності бездротового зв'язку.

1.4 Топологія, архітектура й обладнання мережі Wi-Fi

У світі комп'ютерних мереж існують різноманітні методи з'єднання компонентів мережі. Топологія мережі визначає структуру та спосіб, яким ці компоненти взаємодіють один з одним. Топологія Wi-Fi має значний вплив на продуктивність, надійність і масштабованість мережі. Вибір конкретної топології впливає на ряд аспектів:

- необхідний склад мережевого обладнання;
- можливості самого мережевого обладнання;
- можливості розширення мережі;
- методи управління мережею.

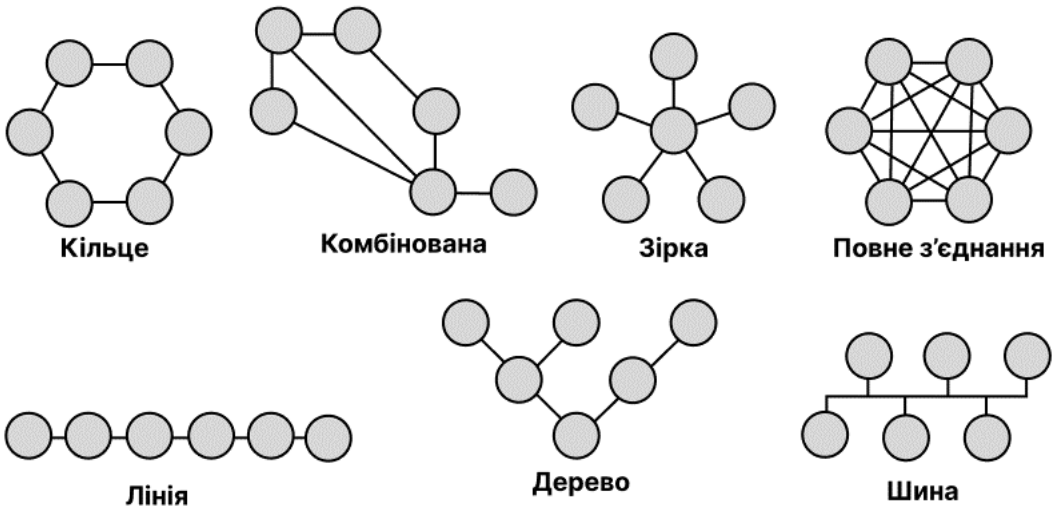

Рисунок 1.1 – Типи топології комп’ютерних мереж

Джерело: розроблено автором на основі [7]

Основні типи топологій мережі Wi-Fi наведені нижче [7, с.44]:

1. Кільцева топологія (Ring). У цій топології кожен пристрій підключений до двох інших пристроїв, утворюючи кільце. Дані обертаються вздовж кільця в одному напрямку.

2. Зіркова топологія (Star). У цій топології всі пристрої підключені безпосередньо до центрального вузла, який може бути точкою доступу Wi-Fi (AP) або маршрутизатором.

3. Комбінована топологія (Hybrid) - це поєднання різних типів топологій. Наприклад, може бути комбінація зіркової топології з деревоподібною.

4. Повне з'єднання (Mesh). У такій топології кожен пристрій мережі може бути підключений до будь-якого іншого пристрою у мережі. Це дозволяє створити мережу з високою надійністю і швидкодією, оскільки дані можуть шляхом оптимального маршруту проходити через різні вузли.

5. Лінійна топологія (Linear). У такій топології всі пристрої підключені один до одного в лінію. Дані передаються від одного кінця до іншого.

6. Деревоподібна топологія (Tree). Ця топологія має ієрархічну структуру, де пристрої підключені у вигляді дерева, з одним центральним вузлом (зазвичай коренем) і різними рівнями вузлів.

7. Шинна топологія (Bus). У цій топології всі пристрої підключені до одного центрального каналу (або "шини"), через який передаються дані.

Архітектура Wi-Fi формує структурну основу бездротової мережі, визначаючи, як пристрої підключаються та взаємодіють у бездротовій мережі. По суті, архітектура Wi-Fi складається з декількох ключових компонентів, включаючи точки доступу (AP), бездротові клієнти та мережеву інфраструктуру.

Точки доступу служать шлюзами, через які пристрої підключаються до мережі, передаючи і приймаючи дані бездротовим способом. Архітектура також охоплює структуру мережі, незалежно від того, чи це одна точка доступу в будинку, чи складна корпоративна мережа з декількома точками доступу, контролерами та розширеними системами управління. Правильно спроектована архітектура Wi-Fi враховує такі фактори, як покриття, пропускна здатність, безпека і масштабованість, щоб забезпечити надійну і ефективну бездротову мережу, яка відповідає конкретним потребам користувачів і додатків.

Існує два основних типи архітектури мереж Wi-Fi.

1. Централізована архітектура (Centralized Architecture).

У централізованій архітектурі усі точки доступу підконтрольовані центральним контролером. Цей контролер відповідає за керування та координацію роботи всіх точок доступу в мережі Wi-Fi. Контролер зазвичай розташований в центральному місці мережі і обробляє всі комутаційні та управляючі функції.

Основні переваги централізованої архітектури:

- просте управління мережею через централізований контролер;
- зручне впровадження змін у конфігурації мережі.

Основні недоліки:

- залежність від центрального контролера, який може бути точкою витоку;
- можлива проблема з підвищенням обсягів трафіку на лінії зв'язку між точками доступу та контролером.

2. Розподілена архітектура (Distributed Architecture).

У розподіленій архітектурі точки доступу працюють автономно, без центрального контролера. Кожна точка доступу приймає рішення щодо маршрутизації трафіку та керування бездротовим зв'язком.

Основні переваги розподіленої архітектури:

- відсутність єдиного пункту витоку для управління та обробки даних;
- зменшення обсягів трафіку на лінії зв'язку, оскільки керування розподілено між точками доступу.

Основний недолік - складніше управління та моніторинг мережі, оскільки керування розподілене між різними точками доступу.

Кожна архітектура має свої застосування в залежності від конкретних умов і вимог мережі. Наприклад, великі корпоративні мережі можуть віддавати перевагу централізованій архітектурі, тоді як розподілена архітектура може бути ефективною для розгалужених мереж або сценаріїв з великою кількістю точок доступу.

Надійний та високопродуктивний Wi-Fi має вирішальне значення для будь-якого сучасного бізнесу. Він забезпечує зв'язок між працівниками, функціонування

пристроїв та задоволення гостей. Але на відміну від домашніх мереж, корпоративний Wi-Fi потребує спеціалізованого обладнання, щоб впоратися з великою кількістю користувачів, різними моделями використання та потенційними проблемами безпеки. Мережеве обладнання повинно не тільки працювати цілий день, але й бути конфігурованим і масштабованим. Таким чином, налаштування та обладнання корпоративної мережі Wi-Fi набагато складніше, ніж типової домашньої мережі Wi-Fi.

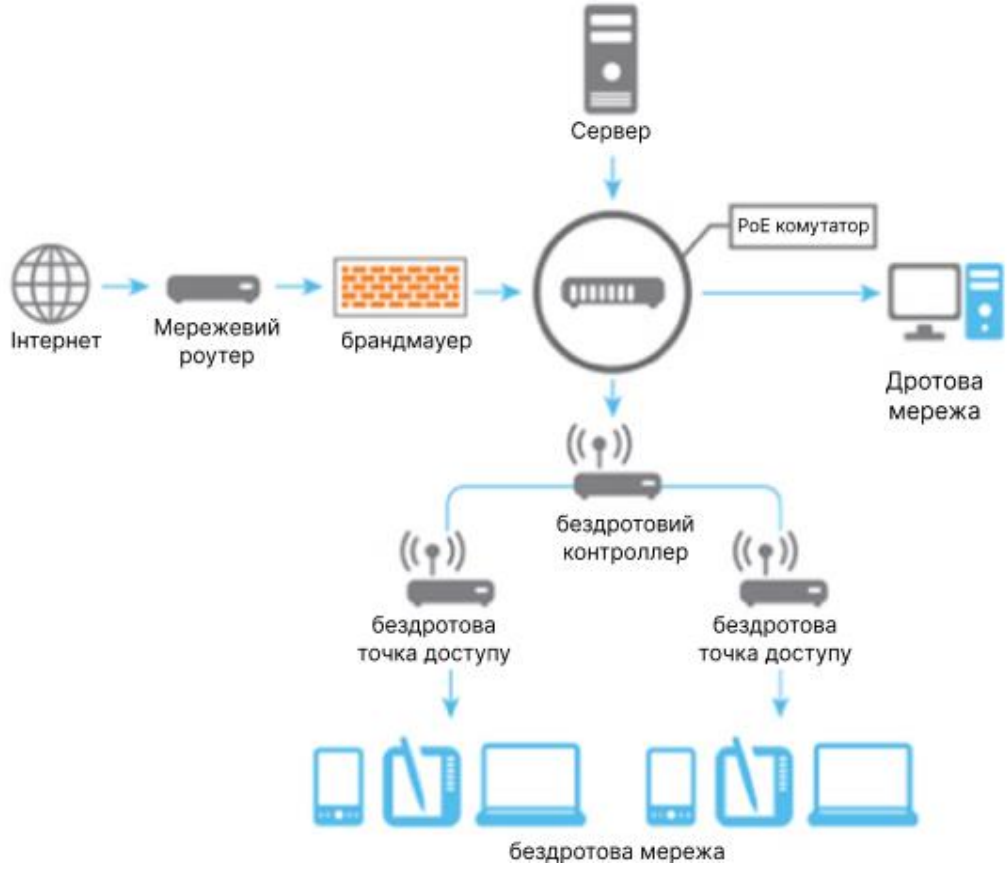

Рисунок 1.2 – Приклад схеми бездротової локальної мережі

Проаналізуємо необхідне мережеве обладнання для корпоративної мережі Wi-Fi [8].

1. Маршрутизатори (роутери). Основна функція полягає в управлінні та маршрутизації трафіку даних по мережі. Він також може використовуватися для підключення кількох локальних мереж одна до одної. Для підприємств важливо мати маршрутизатор, який може обробляти великий обсяг трафіку.

Маршрутизатор працює на третьому рівні моделі мережі osi, використовуючи тип мережі та правила, встановлені адміністратором для передачі пакетів даних, і може виконувати трансляцію адреси одержувача та відправника, а також може фільтрувати трафік пакетів даних для обмеження шифрувати або розшифровувати дані, мережі з використанням комутаторів і маршрутизаторів полягає в тому, що мережа з комутаторами не блокує радіопередачі, тому комутатори можуть бути пошкоджені потоками радіопередачі, маршрутизатори блокують радіопередачі локально в мережі, тому радіотранспорт. потоки впливають лише на свій вихідний домен.

2. Комутатори (Switch). Використовуються для з'єднання різних пристроїв в мережу, таких як комп'ютери, принтери, сервери тощо. Основна функція комутаторів полягає у передачі даних між пристроями в мережі, а також у визначенні того, які пристрої можуть спілкуватися між собою.

Комутатор використовує другий рівень моделі осі, вхідний пакет, що надходить на комутатор, буде надіслано лише одержувачу, що підвищує безпеку, а також продуктивність, на відміну від концентратора, принцип роботи полягає в зберіганні таблиці комутації, яка містить список відповідності групових адрес вузлів портам комутатора.

3. Точка доступу (AP) - це мережевий пристрій, який дозволяє бездротовим пристроям, таким як ноутбуки, смартфони та планшети, підключатися до дротової мережі (LAN) або Інтернету. По суті, вона слугує мостом між бездротовими пристроями та дротовою мережевою інфраструктурою. Вони відіграють вирішальну роль у забезпеченні зручності та гнучкості бездротової мережі, легко інтегруючись з існуючою дротовою інфраструктурою.

4. Фаєрвол(брандмауер) – це система безпеки, яка захищає ваш комп’ютер або мережу від несанкціонованого доступу. Вона діє як бар’єр між вашим комп’ютером та Інтернетом і контролює, які дані можуть входити та виходити. Фаєрволи працюють, відстежуючи та фільтруючи мережевий трафік.

Апаратні брандмауери – це фізичні пристрої, які розміщуються між мережею та Інтернетом. Вони дуже ефективні в забезпеченні безпеки, але їх також може бути дорожче та складніше налаштувати.

Програмні брандмауери – це програми, які працюють на комп’ютерах. . Їх простіше налаштувати та обслуговувати, ніж апаратні брандмауери, але вони також можуть бути менш безпечними.

5. Мережевий міст - це пристрої, що працюють на другому (канальному) рівні моделі OSI (Open Systems Interconnection) і використовуються для з'єднання двох або більше мережевих сегментів, що працюють на одній і тій же фізичній мережі. Основна функція мостів полягає в передачі кадрів даних між цими сегментами на основі їх MAC-адрес. Мережеві мости можуть зменшити навантаження на мережу, фільтруючи пакети даних і сегментуючи мережу. Основним стандартом є бездротова розподільна система (WDS).

6. Мережеві кабелі невід'ємна частина будь-якої локальної мережі (LAN). Вони використовуються для фізичного з'єднання пристроїв, таких як комп'ютери, сервери, маршрутизатори та комутатори, щоб забезпечити передачу даних.

7. Wi-Fi-адаптер – це пристрій, який дозволяє вашому комп’ютеру або іншому пристрою підключатися до бездротової мережі. Існує два типи адаптерів Wi-Fi: внутрішні та зовнішні. Внутрішні адаптери Wi-Fi вбудовані в комп’ютер. Зовнішні адаптери Wi-Fi – це пристрої, які підключаються до комп’ютера через USB-порт.

8. Контролери бездротової мережі - це пристрої, які використовуються для керування та моніторингу бездротових мереж. Контролери бездротової мережі можна використовувати для налаштування параметрів бездротової мережі, усунення несправностей і забезпечення безпеки.

9. Подовжувачі діапазону - це пристрої, які використовуються для розширення діапазону існуючої бездротової мережі. Подовжувачі діапазону підключаються до бездротової мережі та повторюють сигнал, що дозволяє йому охоплювати більшу площу.

Вибір правильного обладнання визначає ефективність та надійність вашої бездротової мережі. Під час вибору обладнання слід звертати увагу на такі параметри, як пропускна здатність, радіус покриття, підтримка стандартів бездротового зв'язку, а також можливості керування та моніторингу. Крім того, важливо враховувати потенційні майбутні потреби мережі та гнучкість управління.

1.5 Аналіз проблем інформаційної безпеки бездротових мереж зв’язку

Бездротові мережі стали невід'ємною частиною сучасного бізнесу, надаючи співробітникам і клієнтам зручний доступ до Інтернету та ресурсів компанії. Однак ці мережі також вразливі до різноманітних загроз, які можуть скомпрометувати конфіденційну інформацію та порушити роботу. Вразливості бездротової мережі - це слабкі місця та прогалини в безпеці бездротової мережі, які можуть бути використані хакерами або неавторизованими користувачами. Ці вразливості є недоліками в дизайні, впровадженні або конфігурації бездротової мережі, які можуть поставити під загрозу її безпеку і зробити її вразливою до кібератак.

Нижче наведено найпоширеніші типи мережевих вразливостей [9, 114-116; 10, 735-736]:

1. Перехоплення даних – це атаки, які передбачають перехоплення бездротового трафіку, дозволяють зловмисникам отримувати конфіденційну інформацію, таку як паролі, особисті дані, фінансові відомості тощо, використовуючи різноманітні методи, такі як "прослуховування" (sniffing).

2. Атаки посередника (Man-in-the-Middle) - у цих атаках зловмисник розташовується між бездротовим клієнтом і легітимною точкою доступу, перехоплюючи і маніпулюючи передачею даних. Потім зловмисник може передавати інформацію, створюючи враження, що він є легітимною точкою доступу. Це дозволяє йому непомітно перехоплювати дані або виконувати інші зловмисні дії.

3. Атаки перебору паролів (Brute Force) — це метод злому паролів, при якому зловмисник намагається підбирати всі можливі комбінації символів, поки не

знайде правильний пароль. Такий метод може бути ефективним, але вимагає значного часу та обчислювальних ресурсів, особливо якщо пароль довгий і складний.

4. Атаки на точки доступу і маршрутизатори. Зловмисники можуть використовувати атаки на безпеку самого обладнання Wi-Fi, такі як атаки з використанням вразливостей програмного забезпечення, атаки з перепрограмування (Firmware Hacking) та фізичний доступ до обладнання.

Зловмисники можуть створити несанкціоновану точку доступу з тим самим SSID, щоб пристрої співробітників, які знаходяться поблизу несанкціонованої точки доступу, автоматично надсилали запити на автентифікацію. Використання протоколу PEAPv0/EAPMsCHAPv2 в поєднанні з неіснуючою або помилковою перевіркою сертифіката точки доступу дозволяє зловмисникам отримати значення Challenge-Response, що використовуються при автентифікації. Озброївшись цими даними, зловмисник може підібрати хеш пароля для легітимної мережі з таким самим SSID.

5. Атаки на відмову в обслуговуванні (DoS). В процесі цієї атаки зловмисники заповнюють бездротовий частотний спектр сигналами перешкод, порушуючи зв'язок між пристроями та точками доступу. Створюючи надмірне навантаження, вони можуть зробити бездротову мережу непридатною для використання користувачами.

6. Злий двійник (Evil Twin) - це тип загрози, коли зловмисник створює фальшиву, незахищену мережу Wi-Fi, яка виглядає як легальна, оскільки використовує той самий SSID. Ця оманлива мережа обманом змушує користувачів підключатися, думаючи, що це надійна точка доступу Wi-Fi.

7. Піггібекінг (Piggybacking) - це різновид соціальної інженерії, коли неавторизована особа отримує доступ до системи з обмеженим доступом або фізичного простору, використовуючи слабкі місця в системі безпеки. Зловмисник використовує облікові дані або права доступу авторизованого користувача, щоб обійти заходи безпеки.

8. Фішинг (Phishing) - маскуючись під авторитетне джерело з привабливим запитом, зловмисник заманює жертву, щоб викрасти конфіденційну інформацію,

зазвичай у вигляді імен користувачів, паролів, номерів кредитних карток, інформації про банківські рахунки або інших важливих даних з метою використання або продажу викраденої інформації.

9. Вразливості протоколів безпеки. Використання застарілих або слабких протоколів шифрування, таких як WEP (Wired Equivalent Privacy), може призвести до вразливостей, які дозволяють зловмисникам легко розшифровувати паролі та іншу конфіденційну інформацію.

10. Внутрішні загрози. Мережа особливо вразлива до зловмисних інсайдерів, які вже мають привілейований доступ до систем організації. Внутрішні загрози може бути важко виявити і захистити від них, оскільки інсайдерам не потрібно проникати в мережу, щоб завдати шкоди.

Загалом, для досягнення своїй цілей хакери використовують перевірені роками методи, кількість яких збільшується із розвитком технологій. Чим складніші системи захисту корпоративних Wi-Fi мереж розробляють компанії, тим досконаліші методи їх зламу винаходять хакери. Ці проблеми підкреслюють необхідність ретельного планування, реалізації та управління безпекою бездротових мереж, а також постійного моніторингу та оновлення заходів захисту.

1.6 Огляд підходів до вирішення проблем інформаційної безпеки в бездротових мережах зв’язку

Вирішення проблем інформаційної безпеки включає в себе застосування різноманітних підходів та стратегій, які спрямовані на захист інформації від загроз та забезпечення безпеки в інформаційному середовищі. Розглянемо деякі ключові підходи до вирішення проблем інформаційної безпеки.

1. Профілактика.

1.1. Шифрування даних забезпечує конфіденційність та цілісність інформації, що передається через мережу або зберігається на пристроях. Використання шифрування може запобігти перехопленню даних та несанкціонованому доступу. Основні методи шифрування в бездротовій мережі розглянуті нижче [11].

Протокол WEP (Дротовий еквівалентний протокол конфіденційності) вважається стандартом для шифрування бездротових мереж. У сучасному світі він все рідше використовується через ризик безпеки, з яким він пов'язаний. WEP не вважається стабільним, і Wi-Fi припинив його використання в 2004 році, оскільки цей рівень безпеки легко зламати.

На зміну WEP прийшов протокол Wi-Fi Protected Access Protocol який забезпечує більшу безпеку і надійність. WPA має 128-бітний динамічний ключ, який важко зламати, що робить його унікальним.

Протокол WPA 2. Протокол з'явився наступним і був кращим за попередні типи шифрування. Тут протокол цілісності тимчасового ключа був замінений на шифрування блочного ланцюжка повідомлень з режимом лічильника. WPA2 пропонує розширені стандарти шифрування (AES). Однак основним недоліком WPA2 є те, що якщо ключ безпеки потрапляє до рук хакера, то вся мережа стає вразливою до атаки.

Протокол WPA3. WPA3 - це новітнє шифрування безпеки, яке набирає популярності. WPA3 забезпечує високий рівень захисту та запобігає несанкціонованому доступу. Неавторизовані та неавторизовані особи не можуть подолати цей рівень безпеки. WPA3 є найбільш підхожим для публічних мереж, оскільки він виконує автоматичне шифрування. Алгоритм шифрування AES-GCM, що використовується в WPA3, забезпечує підвищену безпеку, поєднуючи шифрування і аутентифікацію, гарантуючи цілісність і конфіденційність Wi-Fi зв'язку

Що стосується методу шифрування, то WPA все ще використовує незахищений потоковий шифр WEP RC4, але забезпечує додатковий захист за допомогою TKIP. У той час як WEP і WPA використовували шифрування RC4, WPA2 використовує більш надійний алгоритм шифрування AES-CCMP, так само як і WPA3.

WPA3 забезпечує надійне шифрування з використанням новітніх методів безпеки. У деяких мережах малого бізнесу, що використовують WPA2-Personal, недосконале чотиристоронне рукостискання безпосередньо базувалося на попередньо наданому ключі (PSK), що робить атаки на PSK, такі як KRACK, не

можливими. Хакери можуть зламати паролі WPA2-Personal за допомогою атак грубої сили, в основному підбираючи пароль знову і знову, поки не знайдеться один з них. Режим WPA3-Personal замінює PSK на одночасну автентифікацію рівних (SAE), що усуває залежність від спільних паролів і дозволяє авторизувати пристрої без шкоди для безпеки.

Протокол WPA3-Enterprise. У той час як для режиму WPA3-Enterprise відбувається перехід від 128-бітного рівня безпеки WPA2-Enterprise до 192-бітного [12, 10с.]. Ця функція забезпечує додатковий захист для чутливих до безпеки сфер, таких як уряд, оборона та промисловість. Крім того, WPA3 впроваджує 256-бітний протокол GCM(Galois/Counter Mode) і 384-бітний режим автентифікації хешованих повідомлень (HMAC) з алгоритмом Secure Hash Algorithm, який встановлює послідовну базову лінію безпеки для кращого захисту конфіденційних даних.

Обмін інформацією про аутентифікацію для кожного пристрою і ключами шифрування здійснюється через EAP. EAP (Extensible Authentication Protocol) для підтримки аутентифікації за допомогою сервера аутентифікації і визначає процес інкапсуляції даних EAP, що передаються між клієнтами (запитуючими пристроями) і серверами аутентифікації і завжди реалізується як частина архітектури 802.1x [13, с.168]. Сервер автентифікації автентифікує клієнтів і експортує випадково згенеровані криптографічні ключі у випадку використання методу EAP з похідним ключовим матеріалом.

EAP-TLS вважається золотим стандартом безпеки мережевої автентифікації. EAP-TLS є дуже безпечним і широко використовуваним протоколом автентифікації в мережевих налаштуваннях. В протоколі використовує цифрові сертифікати як для пристроїв, так і для серверів для перевірки ідентичності один одного.

Сертифікати створюються і функціонують за допомогою концепції, яка називається асиметричною криптографією. EAP-TLS часто використовується в бізнес-середовищі, безпечних мережах Wi-Fi та віртуальних приватних мережах (VPN) для захисту даних і підтвердження особи.

В EAP-TLS підхід до автентифікації складається з декількох важливих кроків, кожен з яких допомагає створити безпечне з'єднання:

1. Ініціація. Клієнт звертається до сервера з проханням розпочати автентифікацію EAP TLS.

2. Привітання сервера та сертифікат. Сервер відповідає "Привіт, сервер" і надає свій SSL-сертифікат. Сертифікат SSL сервера містить його відкритий ключ та інші дані.

3. Запит клієнтського сертифіката. Сервер запитує сертифікат автентифікації клієнта. Сервер надсилає повідомлення "Запит на сертифікат клієнта", якщо йому потрібен сертифікат клієнта.

4. Обмін ключами. Клієнти передають SSL-сертифікати серверам. Сертифікат клієнта містить його відкритий ключ та іншу інформацію. Після надсилання сертифіката клієнт і сервер можуть обмінятися ключами для створення спільного секрету.

5. Перевірка сервером. Сервер перевіряє сертифікат клієнта. Він підтверджує сертифікат клієнта і може перевірити CRL або ланцюжок сертифікатів.

6. Перевірка клієнта. Клієнт перевіряє сертифікат сервера так само, як і сервер. Клієнт перевіряє сертифікат сервера.

7. Генерація ключа сеансу. Після автентифікації клієнт і сервер створюють ключ сеансу або набір ключів для шифрування даних.

8. Безпечна комунікація. Після встановлення ключа сеансу клієнт і сервер можуть використовувати TLS для безпечної передачі даних.

1.2. Аутентифікація та авторизація. Ефективна система аутентифікації та авторизації дозволяє контролювати доступ до інформації та ресурсів тільки авторизованим користувачам.

Автентифікація - це акт підтвердження того, що користувачі є тими, за кого себе видають [14, с.81]. Це перший крок у будь-якому процесі безпеки.

Способами автентифікації можуть бути:

- біометрія, коли користувач надає відбиток пальця або сканування ока, щоб отримати доступ до системи;
- одноразові пін-коди, що надають доступ лише на один сеанс або транзакцію;
- додатки для автентифікації, які генерують коди безпеки за допомогою зовнішньої сторони, яка надає доступ;
- паролі. Імена користувачів та паролі є найпоширенішими факторами автентифікації. Якщо користувач вводить правильні дані, система вважає, що ідентифікація дійсна, і надає доступ.

Авторизація в системній безпеці - це процес надання користувачеві дозволу на доступ до певного ресурсу або функції[14, с.150]. Цей термін часто використовується як взаємозамінний з контролем доступу або привілеями клієнта.

Надання комусь дозволу на завантаження певного файлу на сервері або надання окремим користувачам адміністративного доступу до програми є хорошими прикладами авторизації.

У захищених середовищах авторизація завжди повинна слідувати за автентифікацією. Користувачі повинні спочатку довести, що їхні особи справжні, перш ніж адміністратори організації нададуть їм доступ до запитуваних ресурсів.

1.3. Фільтрація трафіку. Використання брандмауерів та інших засобів фільтрації трафіку для блокування небажаного трафіку. Брандмауер – це програмне або апаратне забезпечення, яке контролює вхідний і вихідний трафік у комп’ютерній мережі. Він діє як бар’єр між довіреною та недовіреною мережею, такою як Інтернет. Брандмауери можуть бути налаштовані для дозволу або блокування трафіку на основі низки критеріїв, включаючи IP-адресу, номер порту та тип протоколу.

1.4. Захист за допомогою ПЗ. Антивірус - це програма, призначена для захисту комп'ютера від шкідливого програмного забезпечення (шкідливе ПЗ). Шкідливе ПЗ - це загальний термін для програм, які можуть завдати шкоди вашому комп'ютеру, таким як віруси, трояни, шпигунські програми та рекламне ПЗ.

1.5. Захист периметра. Цей підхід передбачає створення захисного "периметра" навколо інформаційних ресурсів, щоб запобігти несанкціонованому доступу. Це може включати в себе використання:

- VPN (віртуальних приватних мереж) - це інструмент безпеки та конфіденційності, який шифрує ваш інтернет-трафік і тунелює його через захищений сервер, що ускладнює для третіх осіб відстеження вашої активності в Інтернеті, викрадення ваших даних або обмеження вашого доступу до веб-сайтів [15, с.155].

VPN, що означає віртуальна приватна мережа, встановлює цифрове з'єднання між вашим комп'ютером і віддаленим сервером, що належить провайдеру VPN, створюючи тунель "точка-точка", який шифрує ваші особисті дані, маскує вашу IP-адресу і дозволяє вам обходити блокування веб-сайтів і брандмауери в Інтернеті. Це гарантує, що ваша робота в Інтернеті є приватною, захищеною та більш безпечною.

На додаток до шифрування, VPN також маскує вашу IP-адресу від публічного Інтернету, що, в свою чергу, маскує вашу особу. Коли користувач успішно підключає свій комп'ютер до VPN-сервера, VPN не тільки захищає його дані, але й присвоює йому нову IP-адресу, яка приховує його справжню IP-адресу.

Маскування IP-адреси також виявилося ефективним проти доксінгу, коли ваша особиста інформація оприлюднюється в Інтернеті, а також проти DDoS-атак, або розподілених атак на відмову в обслуговуванні.

- Система запобігання вторгненням (IPS) – це пристрій або програмне забезпечення, яке відстежує та блокує підозрілу мережеву активність [16, с.10]. IPS можна розмістити на брандмауері або як окремий пристрій.

IPS працюють, порівнюючи мережеву активність із набором правил. Ці правила визначають, яка активність вважається нормальною, а яка – ні. Якщо IPS виявляє активність, яка порушує правило, він вживає заходів для її блокування. Ці дії можуть включати блокування IP-адреси, скидання пакета або відключення порту.

2. Виявлення.

2.1 Система виявлення вторгнень (IDS) - це програмне або апаратне рішення, призначене для моніторингу мережевого трафіку або активності системи на предмет

підозрілих дій, які можуть бути ознаками вторгнення або атаки [16, с.10]. Вона аналізує вхідні та вихідні дані в реальному часі, застосовуючи різні методи виявлення загроз, такі як сигнатурний аналіз, який порівнює трафік з базою даних відомих атак, або поведінковий аналіз, що виявляє аномалії в нормальній діяльності системи.

IDS може працювати в пасивному режимі, просто виявляючи та реєструючи підозрілі дії, або в активному режимі, повідомляючи адміністратора про потенційні загрози або навіть автоматично реагуючи на них, щоб запобігти можливим атакам.

2.2 Моніторинг та аналіз заходів безпеки: системи моніторингу та аналізу дозволяють виявляти аномальну активність, вразливості та загрози безпеки. Це може включати в себе використання SIEM (систем управління подіями та інформацією безпеки), систем виявлення вторгнень, аналіз журналів подій тощо.

Програмні продукти та послуги SIEM об’єднують в собі кілька різних технологій [17, с.143]:

LMS «Log Management System» - це система, яка автоматично збирає та зберігає файли журналів з різних джерел, таких як операційні системи та додатки, у централізованому сховищі. Це дозволяє забезпечити зручний та однаковий доступ до журналів з будь-якого хосту чи системи.

SLM/SEM «Security Log/ Event Management» - ці системи забезпечують активний моніторинг та аналіз подій безпеки, включаючи їх візуалізацію та надсилання повідомлень про потенційні загрози.

SIM «Security Information Management» - це система, спрямована на збір та управління інформацією щодо безпеки з різних джерел, що дозволяє ефективно керувати безпековими даними.

SEC «Security Event Correlation» - ця система визначає та корелює події безпеки, що дозволяє ідентифікувати та реагувати на потенційні загрози.

3. Реагування.

3.1 Відновлення даних. Регулярне резервне копіювання даних та наявність планів відновлення дозволяють підприємствам відновлювати доступ до даних в разі їх втрати або пошкодження.

3.2 Аналіз інцидентів включає визначення причини та наслідків інциденту інформаційної безпеки, що дозволяє ідентифікувати вразливості в системі та вжити відповідних заходів для запобігання подібним інцидентам у майбутньому.

4. Постійне вдосконалення.

4.1 Регулярне оновлення програмного забезпечення, що використовується в бездротових мережах, для усунення вразливостей допомагає захистити систему від нових загроз, зменшуючи ризик експлуатації відомих недоліків хакерами.

4.2 Навчання персоналу практик безпеки, таких як необхідність складних паролів, уникання кліків по невідомих посиланнях та підозрілих вкладеннях, може значно знизити ризики безпеки.

Важливо зазначити, що жоден метод захисту не є досконалим. Для забезпечення максимальної безпеки вашої бездротової мережі важливо використовувати комбінацію різних методів.

1.7 Висновки до першого розділу

Технологія Wi-Fi забезпечує бездротовий доступ до мережі за допомогою радіохвиль. Принцип роботи полягає в передачі даних між пристроями через бездротові канали на основі стандартів IEEE 802.11.

Стандарти Wi-Fi визначають технічні параметри бездротового зв'язку. Мережа Wi-Fi складається з точок доступу, маршрутизаторів, клієнтських пристроїв та інших компонентів, які взаємодіють між собою для забезпечення безперервного зв'язку.

Аналіз можливостей технології бездротового зв’язку Wi-Fi для побудови корпоративних локальних мереж свідчить про її значний потенціал та переваги для сучасних бізнесів. Wi-Fi технологія забезпечує зручний доступ до мережі для співробітників, підвищує мобільність та продуктивність роботи, а також дозволяє підприємствам ефективно впроваджувати інноваційні рішення в галузі IT.

Однак безпека залишається однією з ключових проблем у використанні бездротових мереж у корпоративному середовищі. Потенційні загрози, такі як

перехоплення даних, атаки на аутентифікацію та вразливості протоколів безпеки, вимагають відповідного захисту та ретельного аналізу безпеки.

Огляд різноманітних підходів до вирішення проблем безпеки вказує на необхідність комплексного підходу, що включає в себе шифрування, аутентифікацію, моніторинг та інші заходи безпеки. Впровадження цих заходів разом з відповідністю нормативним вимогам дозволить підприємствам максимально забезпечити безпеку своїх бездротових корпоративних мереж.

РОЗДІЛ 2. ПЛАНУВАННЯ ТА РОЗГОРТАННЯ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ WI-FI

Професійно спланована та належно розгорнута Wi-Fi мережа може забезпечити високу швидкість передачі даних, надійність з'єднання та забезпечити мобільність співробітників, що є критичним для підвищення продуктивності та конкурентоспроможності підприємства.

У цьому підрозділі буде розглянуто процес розробки структурної схеми бездротової мережі Wi-Fi, включаючи розташування точок доступу, клієнтських пристроїв та іншого обладнання для оптимального покриття та функціональності мережі. Буде проведено аналіз та обґрунтування вибору обладнання для Wi-Fi мережі, включаючи точки доступу, маршрутизатори, комутатори та інше обладнання, з урахуванням потреб корпоративного середовища та технічних вимог. Буде надано методику та процес розрахунку зон покриття Wi-Fi обладнання з метою оптимізації розташування точок доступу та забезпечення необхідного покриття та пропускної здатності.

Зрозуміння цих аспектів дозволить забезпечити стабільну та ефективну роботу Wi-Fi мережі, що в свою чергу позитивно позначиться на робочих процесах, сприятиме зростанню ефективності співробітників та сприяти відкриттю нових можливостей для розвитку бізнесу.

2.1 Розробка структурної схеми Wi-Fi мережі

В сучасному корпоративному середовищі розробка ефективної Wi-Fi мережі є стратегічно важливим завданням для забезпечення високошвидкісного та надійного бездротового зв'язку. Структурна схема Wi-Fi мережі є ключовим компонентом цього процесу, оскільки вона визначає організацію та взаємозв'язки між різними компонентами мережі.

Структурна схема Wi-Fi мережі - це візуальне представлення її компонентів та їх взаємозв'язків. Вона використовується для документування мережі, планування її розширення та усунення несправностей.

Розробка та впровадження Wi-Fi мережі включає декілька етапів.

Етап 1. Планування та оцінка.

Зона покриття.

Одним з основних моментів при проектуванні бездротової мережі є визначення зони покриття. Зона покриття визначає, де користувачі можуть отримати доступ до мережі. Такі фактори, як розмір будівлі, планування і перешкоди (стіни і меблі) повинні бути ретельно проаналізовані, щоб гарантувати, що мережа буде охоплювати всі необхідні зони. Проведення обстеження об'єкта може допомогти виявити мертві зони та оптимізувати покриття.

Через природу поширення радіочастот, випромінювання радіосигналу, як правило, не можна обмежити в межах певної будівлі або місця. Надмірне покриття бездротового сигналу може становити значну загрозу для організації, відкриваючи її для зовнішніх атак на мережу. Тому на етапі планування мережі необхідно добре розуміти вимоги до покриття бажаної бездротової мережі. Виконуючи обстеження об'єкта, можна визначити:

- відповідні технології для застосування;
- перешкоди, яких потрібно уникнути, усунути або обійти;
- моделі покриття, які слід прийняти;
- необхідну пропускну здатність.

Стандарти бездротового зв'язку.

З моменту появи стандарту 802.11 постійно вносяться вдосконалення, спрямовані на підвищення швидкості передачі даних, дальності дії сигналу та безпеки бездротових мереж. Тому корисно відстежувати розвиток нових стандартів по мірі їх появи, зокрема, при купівлі нового обладнання або придбанні нових послуг бездротової мережі. Вибір відповідного стандарту бездротового зв'язку для ваших

вимог до підключення та оптимальної продуктивності мережі є дуже важливим. Найпоширенішими стандартами на сьогодні є Wi-Fi 5 (802.11ac) і Wi-Fi 6 (802.11ax).

Тому потрібно звернути увагу щоб кожен компонент мережевої інфраструктури, включаючи маршрутизатори, точки доступу і клієнтські пристрої, сумісний з обраним стандартом.

Планування каналів.

Ефективне планування каналів може суттєво вплинути на продуктивність бездротової мережі. Перекриття каналів може призвести до перешкод і зниження пропускної здатності. Необхідно проаналізувати доступні канали та використовувати інструменти для виявлення перешкод і вибору найменш перевантажених каналів. Динамічне призначення каналів також може допомогти оптимізувати продуктивність, автоматично налаштовуючи канали відповідно до умов мережі.

Безпека.

Бездротові мережі вразливі до загроз безпеки, тому впровадження надійних заходів безпеки має першорядне значення. Рекомендується використовувати надійні протоколи шифрування, для захисту даних під час передачі, надійні, унікальні паролі для точок доступу та регулярно оновлювати їх.

Концепція "глибинного захисту" широко використовується в захищеному проектуванні дротових мереж. Ця ж концепція може бути застосована і до бездротових мереж. Завдяки впровадженню декількох рівнів захисту, ризик вторгнення через бездротову мережу значно знижується. Якщо зловмисник порушує один із заходів, для захисту мережі залишаються додаткові заходи та рівні безпеки.

Також гарною ідеєю буде сегментація мережі, щоб ізолювати конфіденційні дані від загального доступу. Розділення бездротових і дротових сегментів мережі, використання надійних методів автентифікації пристроїв і користувачів, застосування мережевої фільтрації на основі адрес і протоколів, а також розгортання систем виявлення вторгнень в бездротових і дротових мережах - все це можливі заходи, які можуть бути використані для побудови багаторівневого захисту.

Етап 2. Проектування та впровадження мережі.

Ємність і пропускна здатність.

Враховується кількість користувачів і пристроїв, які будуть підключатися до мережі. Мережа має достатню пропускну здатність і смугу пропускання, щоб впоратися з очікуваним навантаженням. Для цього може знадобитися розгортання декількох точок доступу, щоб рівномірно розподілити трафік і запобігти перевантаженню. Перед проектуванням бездротової мережі важливо зрозуміти бізнес та функціональні вимоги до бездротового рішення. Ці вимоги можуть вплинути на рішення про те, які заходи безпеки слід розгорнути для захисту мережі. Наприклад, якщо потрібен гостьовий доступ, на етапі проектування слід врахувати найкращі практики безпеки для гостьового доступу.

Якість обслуговування (QoS).

Налаштування QoS визначають пріоритетність трафіку в мережі, гарантуючи, що критично важливі програми отримують достатню пропускну здатність. Це особливо важливо в середовищах, де використовуються відеоконференції, VoIP-дзвінки та інші програми, що працюють у режимі реального часу. Призначаючи вищий пріоритет цим програмам, можна підтримувати стабільну роботу користувачів.

Резервування і масштабованість.

Масштабованість гарантує, що мережа зможе вмістити додаткових користувачів і пристрої в міру зростання організації. Резервування, з іншого боку, забезпечує варіанти резервного копіювання на випадок апаратних збоїв. Резервні точки доступу та інтернет-з'єднання допомагають підтримувати доступність мережі.

Управління та моніторинг.

Інструменти управління та моніторингу мережі для обслуговування та усунення несправностей бездротової мережі. Ці інструменти дозволяють відстежувати продуктивність, виявляти проблеми та віддалено налаштовувати пристрої. Регулярний моніторинг мережі допоможе виявити та вирішити будь-які проблеми до того, як вони вплинуть на користувачів.

Оцінювання та аудит безпеки є важливими засобами для перевірки стану безпеки бездротової мережі та визначення будь-яких коригувальних дій, необхідних для підтримання прийнятного рівня безпеки. Ці оцінки можуть допомогти виявити лазівки в бездротовій мережі, такі як погано налаштовані точки доступу, що використовують стандартні або легко вгадувані паролі, а також наявність або відсутність шифрування. Однак оцінка ризиків безпеки може дати лише загальне уявлення про ризики для інформаційних систем на певний момент часу. Тому важливо регулярно проводити оцінку та аудит після того, як бездротова мережа запущена в експлуатацію.

Таблиця 2.1 - Вимоги до проектування корпоративної бездротової мережі

Розмір та розташування		
Характеристика	**Опис**	**Приклад**
Площа покриття	Вкажіть загальну площу, яку потрібно охопити мережею Wi-Fi.	50 квадратних метрів
Кількість поверхів	Вкажіть, скільки поверхів буде охоплювати мережа.	2
Розташування точок доступу	Вкажіть, де будуть розміщені точки доступу Wi-Fi.	1 на кожному поверсі
Розділення мережі	Розділення на віртуальні мережі (VLAN) для підвищення безпеки та керування трафіком	Розділення користувачів на власні VLAN залежно поверху
Обладнання		
Стандарт Wi-Fi	Виберіть стандарт Wi-Fi (наприклад, 802.11ac, 802.11ax).	802.11ax
Тип маршрутизатора	Виберіть тип маршрутизатора (наприклад, односмуговий, двосмуговий).	Двосмуговий
Кількість точок доступу	Вкажіть, скільки точок доступу Wi-Fi вам знадобиться.	2
Тип антени	Виберіть тип антени (наприклад, всеспрямована, спрямована).	Всеспрямована
Кількість користувачів		

Продовження табл. 2.1

Кількість одночасних користувачів	Вкажіть, скільки користувачів одночасно підключатимуться до мережі.	Не менше 20
Типи пристроїв	Вкажіть, які типи пристроїв підключатимуться до мережі	Комп'ютери, ноутбуки, принтери
Безпека		
Шифрування	Виберіть протокол шифрування	WPA3-Enterprise з Алгоритмом шифрування AES-GCM
Пароль	Вкажіть складний пароль для мережі Wi-Fi.	Пароль з 12 символів, що містить цифри, букви та символи. Оновлення паролю кожні 6 місяців.
Гостьова мережа	Створіть окрему мережу Wi-Fi для гостей.	Так
Брандмауера	Встановлення брандмауера для контролювання трафіка у мережі та блокування небажаного доступу до неї зовнішніми джерелами.	Так
Використання механізму аутентифікації	Забезпечення індивідуальної аутентифікації для кожного користувача, що підвищує безпеку мережі та унеможливлює атаки типу "перехоплення" трафіку.	802.1X + RADIUS з протоколом автентифікації EAP-TLS
Моніторинг	Система відстеження активності та виявлення аномальних подій у мережі	Хмарна система AZURE/ AWS

Оптимальною топологією мережі буде зіркова. Ця топологія є найпростішою і найнадійнішою. Вона використовує центральний маршрутизатор, до якого підключені всі інші пристрої.

Обґрунтування:

- ця топологія забезпечує гнучкість та масштабованість;

- легко додати нових користувачів або пристрої;
- забезпечує хороше покриття Wi-Fi на обох поверхах;

Для даної кооперативної мережі Wi-Fi рекомендується використовувати розподілену архітектуру оскільки:

- мережа охоплює 1-й та 2-й поверхи будівлі, розподілити точки доступу між цими поверхами забезпечить краще покриття та ефективніше використання ресурсів;
- розподіл функцій між точками доступу на кожному поверсі дозволить розділити трафік між ними, зменшуючи завантаження на головному маршрутизаторі;
- розподіл функцій між ближчими точками доступу допоможе забезпечити кращу пропускну здатність та швидкість передачі даних на кожному поверсі;
- зменшення впливу відмови: якщо одна точка доступу відмовляє, інші точки доступу все ще продовжують працювати, забезпечуючи доступ до мережі для користувачів.

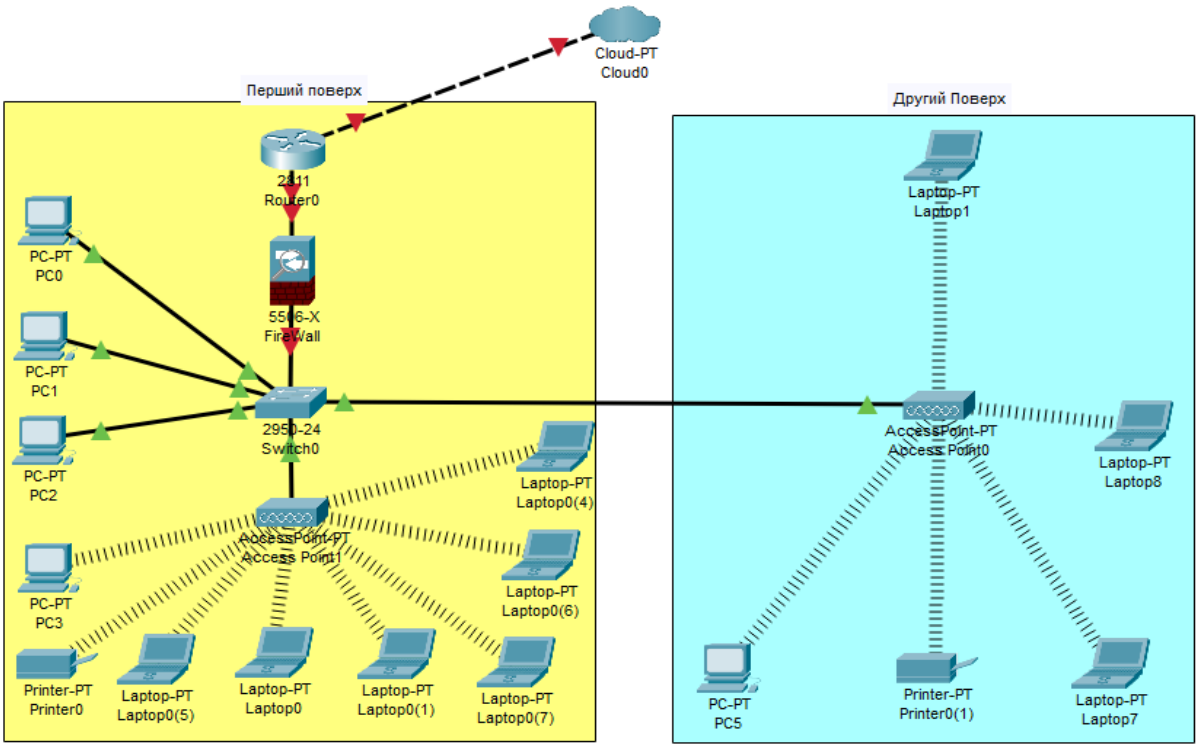

Рисунок 2.1 - Графічна схема Wi-Fi мрежі виконана в програмному забезпеченні Cisco Packet Tracer

Точки доступу розташовані стратегічно в мережі для забезпечення оптимального покриття бездротового сигналу. Клієнтські пристрої вказані як пристрої, що підключаються до бездротової мережі через точки доступу.

Таблиця 2.2 - Структурна схема Wi-Fi мережі

1 Поверх		**2 Поверх**
Пристрої	**Коментар**	**Пристрої**
Маршрутизатор	Для керування трафіком між бездротовими пристроями і провідною мережею, забезпечуючи ефективне маршрутизацію даних та безпеку мережі	
Брандмауер	Для фільтрації шкідливого та потенційно небезпечного контенту та з'єднань	
Комутатор	Для розширення кількості доступних портів	
4 ПК	1ПК - Підключено до точки доступу з вбудованим мережевим адаптером 3ПК – Підлючено кабелем UTP Cat.6	1 ПК
6 Ноутбуків	Підключено до точки доступу	3 Ноутбуки
Принтер. Підключено до точки доступу за допомогою вбудованого мережевого адаптера		
Патч-корди UTP Cat.6. Для підключення маршрутизатора, комутатора, Wi-Fi точок доступу та інших пристроїв		
Точка доступу – 2 Ггц та 5 Ггц		

2.2 Обґрунтування та вибір обладнання

Обґрунтування та вибір обладнання для забезпечення інформаційної безпеки в корпоративній локальній мережі на основі технології Wi-Fi важливі завдання для будь-якої компанії, оскільки безпека даних є пріоритетом у сучасному бізнес-середовищі.

Нижче подано кілька ключових аспектів, які слід врахувати при виборі обладнання для забезпечення безпеки в такій мережі, а також пропозиції щодо вибору відповідного обладнання:

Точки доступу (ТД):

- ТД з підтримкою стандарту Wi-Fi 6 (802.11ax) забезпечують кращу швидкість, надійність та безпеку;
- ТД з підтримкою технології MU-MIMO (Multi-User Multiple Input, Multiple Output) дозволяють одночасно обслуговувати більше клієнтів без зниження продуктивності;
- ТД з функцією гостьового доступу дозволяють надавати доступ до Інтернету гостям без ризику для корпоративної мережі.

Таблиця 2.4 – Характеристики точки доступу Ubiquiti UniFi U6 PRO [18]

Точка доступа Ubiquiti UniFi U6 PRO	
Частота роботи Wi-Fi	5 ГГц + 2.4 ГГц
Особливості	Підтримання PoE MU-MIMO
Стандарт зв'язку Wi-Fi	Wi-Fi 6 (802.11ax)
Швидкість Wi-Fi, Мбіт/с	5400 Мбит/с

Маршрутизатор:

- маршрутизатори з вбудованим брандмауером дозволяють блокувати небажані пакети та захищати мережу від атак;
- маршрутизатор з функцією гостьової мережі;
- маршрутизатори з підтримкою VPN (Virtual Private Network) дозволяють організувати безпечний віддалений доступ до корпоративної мережі;
- маршрутизатори з функцією QoS (Quality of Service) дозволяють пріоритезувати трафік та забезпечувати безперебійну роботу критичних додатків.

Таблиця 2.3 – Характеристики Маршрутизатора ASUS RT-AX88U Pro[19]

Маршрутизатор ASUS RT-AX88U Pro	
Частота роботи Wi-Fi	5 ГГц + 2.4 ГГц (дводіапазонний)
Швидкість LAN портів	2.5 Гбіт/сек
Стандарт зв'язку Wi-Fi	Wi-Fi 6 (802.11ax)
Швидкість Wi-Fi, Мбіт/с	6000 Мбіт/сек
Особливості	Підтримка VPN Пріоритезація трафіку (QoS)
Функції безпеки	Гостьовий доступ Захист від DoS-атак Міжмережевий екран SPI

Мережеві комутатори:

- вибирайте комутатори з Gigabit Ethernet або SFP+ портами для забезпечення високої пропускної здатності;
- підтримка PoE, якщо в мережі присутні точки доступу Wi-Fi, IP-камери або інші пристрої, які потребують живлення через Ethernet-кабель;
- комутатор повинен мати вбудовані засоби захисту від атак, такі як фільтрація мережевого трафіку, контроль доступу, захист від мережевих атак.

Таблиця 2.5 – Характеристики Комутатора TP-LINK TL-SG3210XHP-M2[20]

Комутатор TP-LINK JetStream TL-SG3210XHP-M2	
Кількість і тип портів Ethernet	8 х портів 2.5G Ethernet 2 х портів SFP+
Швидкість LAN портів	2.5 Гбіт/сек
Безпека	Список управління доступом (ACL), безпека портів, захист від DoS-атак, DHCP Snooping, 802.1X, аутентифікація RADIUS та інше.
Додатково	Пріоритизація (QoS) рівня 2/3/4 та IGMP snooping.

Вибір найкращого файерволу для корпоративної мережі важливий для забезпечення безпеки та захисту від загроз зовнішніх атак, внутрішніх порушень безпеки та інших потенційних загроз. Ключові характеристики, які слід врахувати під час вибору найкращого файерволу:

- файервол повинен мати здатність виявляти та блокувати загрози в реальному часі, включаючи віруси, шкідливі програми, вторгнення та інші атаки;
- якщо корпоративна мережа використовує віртуальні приватні мережі (VPN) для забезпечення безпеки віддаленим працівникам, файервол повинен підтримувати різні протоколи VPN та забезпечувати безпеку передачі даних;
- функція автоматичного оновлення загроз дозволяє файерволу автоматично отримувати та застосовувати оновлення підписів для виявлення нових загроз безпеки;

Cisco Secure Firewall 3100 ASA - це високопродуктивний брандмауер, призначений для забезпечення безпеки мереж середнього та великого підприємства.

Cisco Secure Firewall 3100 оснащено високопродуктивним процесором і спеціальним програмним забезпеченням, що забезпечує високу пропускну здатність і швидкість навіть за інтенсивного мережевого трафіку.

Ці брандмауери пропонують широкий спектр функцій безпеки, включаючи виявлення та запобігання вторгненню в Інтернет (IDS/IPS), фільтрацію вмісту, захист від зловмисного програмного забезпечення, а також можливості контролю доступу та автентифікації.

2.3 Розрахунок зон покриття Wi-Fi обладнання

Перед встановленням Wi-Fi мережі важливо розрахувати зону покриття, щоб забезпечити якісний сигнал у всіх потрібних місцях.

Нижче наведені основні кроки для розрахунку зон покриття Wi-Fi мережі:

1. Створення плану приміщення. Важливо врахувати розміри кожного приміщення, розташування стін, перешкод та інших факторів, які можуть впливати на сигнал Wi-Fi.

2. На основі аналізу географічних особливостей приміщення потрібно визначти оптимальне розташування точок доступу. Зазвичай точки доступу розташовуються в центрі кожного приміщення для оптимального покриття.

3. Налаштування параметрів точок доступу, такі як потужність сигналу, канал передачі даних, режим роботи тощо, з урахуванням розрахунків покриття.

4. Моделювання покриття Wi-Fi за допомогою програмного забезпечення для моделювання покриття Wi-Fi на основі встановлених точок доступу та їх параметрів. Програмне забезпечення надасть візуальну інформацію про зони покриття та сигналу Wi-Fi в кожному приміщенні.

5. Після моделювання можуть з'явитися області з недостатнім покриттям сигналу. В таких випадках потрібно розглянути встановлення додаткових точок доступу для покращення покриття.

Фактори, що впливають на зону покриття:

- перешкоди, такі як стіни, меблі та інші об'єкти можуть поглинати або відбивати сигнали Wi-Fi, що зменшує зону покриття;
- інтерференція - інші мережі Wi-Fi та пристрої, такі як мікрохвильові печі та бездротові телефони, можуть створювати перешкоди для сигналів Wi-Fi;
- матеріали будівлі - будівлі з товстими стінами або металевими каркасами можуть значно зменшити зону покриття;
- тип антени - всенаправлені антени забезпечують покриття на 360 градусів, а спрямовані антени фокусують сигнал у певному напрямку;
- потужність передачі;
- чутливість приймача.

Вимірювання рівнів сигналів і шумів з відображенням на плані поверху. З використанням різних наявних апаратно-програмних комплексів, призначених для експериментального планування мереж Wi-Fi, на план об'єкта, що проектується,

наносять рівні сигналів, що приймаються термінальними пристроями від точок доступу, а також контролюють при цьому рівні шумів у каналі. В роботі буде використовуватися додаток NetSpot.

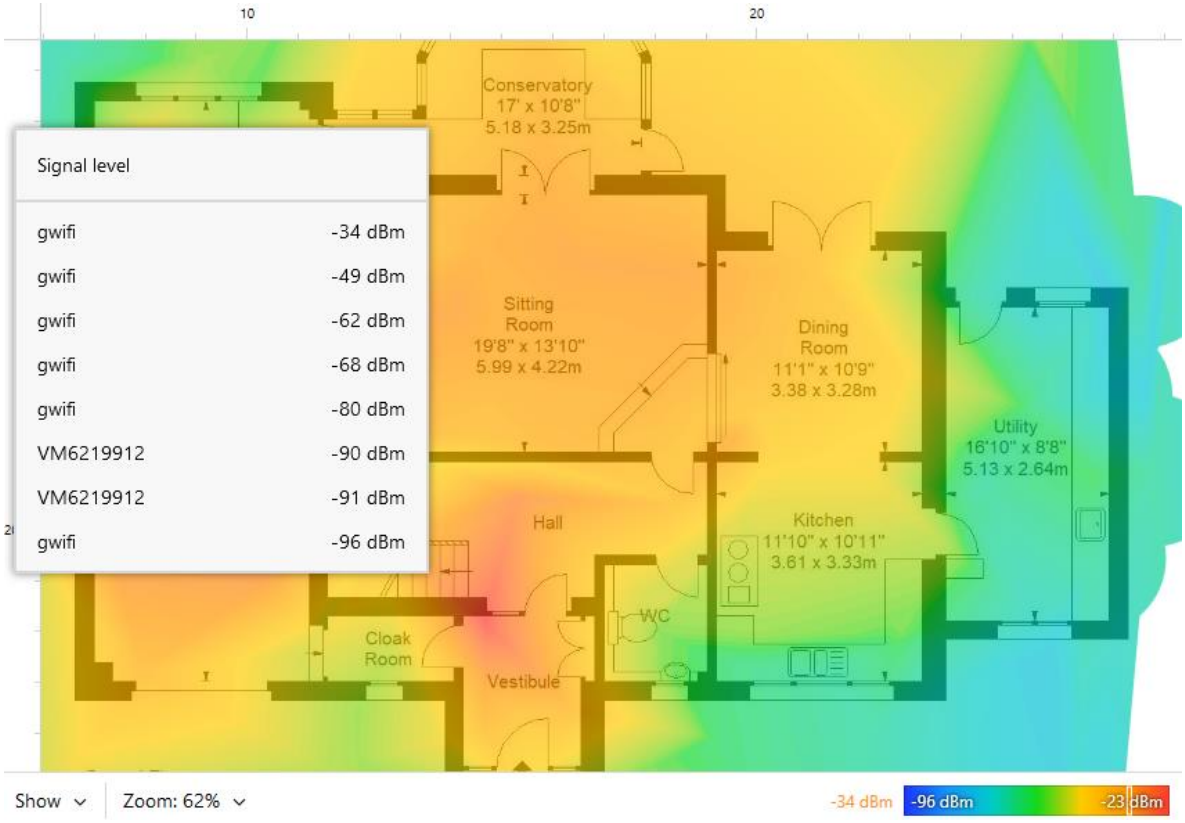

Рисунок 2.2 - Результати експериментальних вимірювань зони покриття бездротової мережі

На діаграмі представлені дані про силу сигналу Wi-Fi на різних ділянках приміщення або області, що були виміряні та аналізовані.

Цей графік відображає реальні умови покриття бездротової мережі в обраному середовищі та може бути використаний для оцінки ефективності розташування точок доступу, виявлення слабких зон покриття та розробки оптимальної конфігурації мережі.

Формула поширення сигналів Wi-Fi у вільному просторі [21]:

$$FSPL = 20 \log_{10}(d) + 20 \log_{10}(f) - 147.55, \quad (1.1)$$

Де FSPL – втрати сигналу у вільному просторі (дБ),

d – відстань між передавачем і приймачем (м),

f – частота сигналу (Гц).

Загальна формула для оцінки зони покриття [21]:

$$RSSI = P_t + G_t + G_r - FSPL, \quad (1.2)$$

Де RSSI – отримана потужність сигналу (дБ),

Pt – передана потужність сигналу (дБ),

Gt – посилення передавальної антени (дБ),

Gr – посилення приймальної антени (дБ),

FSPL – втрати сигналу у вільному просторі (дБ).

Потужність передавача точки доступу P_t становить 20 дБм (100 мВт), посилення антени точки доступу G_t та приймачів G_r - 2 дБ, частота сигналу - 2.4 ГГц.

Для розрахунку втрат у вільному просторі на відстані 50 м:

$FSPL = 20 \log_{10}(50) + 20 \log_{10}(2.4*10^9) - 147.55 = 74.03$ дБ

Отже, загальна потужність сигналу на відстані 50 м (без перешкод):

$RSSI = 20 + 2 + 2 – 74.03 = −50.03$ дБм

Оцінка покриття між поверхами.

Втрати сигналу через залізобетон можуть бути дуже значними. Приблизні втрати для 2.4 ГГц становлять близько 25 дБ.

RSSI = -50.03 - 25 = -75.03 дБм - покриття між поверхах

Це значення є на межі прийнятного для більшості Wi-Fi адаптерів. Тому необхідно встановити Wi-Fi точку доступу на 1-му та 2-му поверсі в центральному місці для забезпечення максимального покриття, враховуючи втрати сигналу через залізобетонне перекриття.

Оцінка покриття на поверхах.

Втрати сигналу через газоблоки для 2.4 ГГц становлять близько 8 дБ в залежності від щільності матеріалу.

RSSI = -50.03 - 8 = −58.3 дБм

Це значення є прийнятним для більшості Wi-Fi адаптерів.

Таким чином, для забезпечення оптимального покриття та продуктивності мережі, необхідно врахувати матеріали будівлі, відстань між пристроями та встановити додаткові точки доступу при необхідності. Також важливо забезпечити налаштування Wi-Fi точок доступу на різних каналах, щоб уникнути перешкод і покращити продуктивність мережі.

2.4 Розрахунок IP-адрес та планування каналів

Розрахунок IP-адрес та планування каналів є важливим аспектами проектування корпоративної мережі. Кожен пристрій у мережі повинен мати унікальну IP-адресу. Коректне призначення адрес допомагає уникнути конфліктів і забезпечує правильне маршрутизацію пакетів.

Для розрахунку IP-адрес в Wi-Fi мережі необхідно виконати кілька кроків. Для цього потрібно:

1. Почніть з вибору маски підмереж, яка відповідатиме потребам конкрутної мережі. Наприклад, часто використовується маска /24 (або 255.255.255.0), що дозволяє до 254 користувачів у кожній підмережі (одна адреса використовується для мережевого пристрою, а інша - для мережевого шлюзу).

2. Налаштування IP-адреси для всіх пристроїв у мережі, включаючи точки доступу, маршрутизатори, сервери і комп'ютери. Пам'ятайте, що IP-адреси повинні бути унікальними в межах кожної підмережі.

3. Зазвичай рекомендується резервувати IP-адреси для критичних пристроїв, таких як сервери або мережеві принтери, щоб уникнути конфліктів із статичними IP-адресами.

4. Налаштуйте DHCP-сервер для автоматичного призначення IP-адрес користувачам. Визначте діапазони IP-адрес, які будуть роздаватися DHCP-сервером.

5. Запишіть всі назначені IP-адреси та іншу важливу інформацію (наприклад, маски підмереж, шлюзи тощо) в документацію вашої мережі. Це полегшить підтримку та управління вашою мережею у майбутньому.

Важливо також враховувати безпеку мережі під час розподілу IP-адрес, забезпечуючи, щоб критичні пристрої мали захищені IP-адреси, і уникнути використання публічних IP-адрес внутрішніх пристроїв.

Для маски 255.255.255.0, всі перші три октети (24 біти) вже використовуються для ідентифікації мережі, тому лишаються лише 8 бітів для підмережі. Але ми маємо створити дві підмережі, тому потрібно використовувати додаткові біти. Для створення двох підмереж за кількістю поверхів і розробки IP-адрес для користувачів, використаємо підмережі класу С з мережовою маскою /24 (255.255.255.0) [22]. Всього доступно 254 IP-адреси для користувачів в кожній підмережі (256 - 2 (IP-адреса мережі та шлюза)).

Загальна кількість пристроїв для першої підмережі - 11 (4 ПК + 6 ноутбуків + принтер); для другої підмережі - 5 (ПК + 3 ноутбуки + принтер).

Для створення двох підмереж із заданої мережі 192.168.255.0 з маскою підмережі 255.255.255.0, нам потрібно розділити цю мережу на дві частини. Це можна зробити за допомогою зміни маски підмережі з /24 на /25. Це дасть нам дві підмережі, кожна з яких матиме по 126 доступних IP-адрес для користувачів.

Тепер призначимо біти підмережі.

Перша підмережа: 192.168.255.0/25 (маска 255.255.255.128)

Друга підмережа: 192.168.255.128/25 (маска 255.255.255.128)

Отже, ми маємо наступні IP-адреси для пристроїв:

1. Перша підмережа (1-й поверх):
   - мережа: 192.168.255.0/25;
   - діапазон адрес: 192.168.255.1 - 192.168.255.126 (126 адрес вільних);
   - широкомовна адреса: 192.168.255.127.

Використані адреси:

   - ПК: 192.168.255.1 - 192.168.255.4;
   - ноутбуки: 192.168.255.5 - 192.168.255.10;
   - принтер: 192.168.255.11.

2. Друга підмережа (2-й поверх):

- мережа: 192.168.255.128/25;
- діапазон адрес: 192.168.255.129 - 192.168.255.254 (126 адрес вільних);
- широкомовна адреса: 192.168.255.255.

Використані адреси:

- ПК: 192.168.255.129;
- ноутбуки: 192.168.255.130 - 192.168.255.132;
- принтер: 192.168.255.133.

Тут використовується діапазони з вільними адресами. Якщо є потреба в додаткових адресах, вони можуть бути використані з вільного діапазону.

Однією з найпоширеніших помилок, яких припускаються підприємства та організації при розгортанні бездротової мережі, є налаштування всіх точок доступу на використання одного каналу Wi-Fi. Такі компанії та організації зазвичай стикаються з великими проблемами з пропускною здатністю, оскільки всі дані проходять через один канал з обмеженою пропускною здатністю.

Метою має бути забезпечення безперебійного роумінгу за рахунок перекриття покриття стільникових мереж, одночасно уникаючи перекриття частотного простору, що може призвести до уповільнення швидкості мережі. Щоб досягти цієї мети, необхідно визначити покриття кожної точки доступу і розташувати їх таким чином, щоб вся територія була покрита з достатнім перекриттям для безперешкодного роумінгу.

Плануючи розгортання бездротової мережі, що складається з декількох точок доступу, важливо враховувати наявність багатоканальної інтерференції [23, с.92-93].

Незважаючи на велику кількість доступних бездротових каналів, не всі вони придатні для використання. Причина криється в частковому перекритті частот. В діапазоні 2.4 ГГц неперекриваються тільки три частоти: 1, 6 і 11.

Вибір, наприклад, каналу № 3 призведе до того, що на нього впливатимуть точки доступу, які працюють на першому і на шостому каналах. І хоча на самому третьому каналі немає жодних інших точок доступу, працювати на ньому буде практично неможливо.

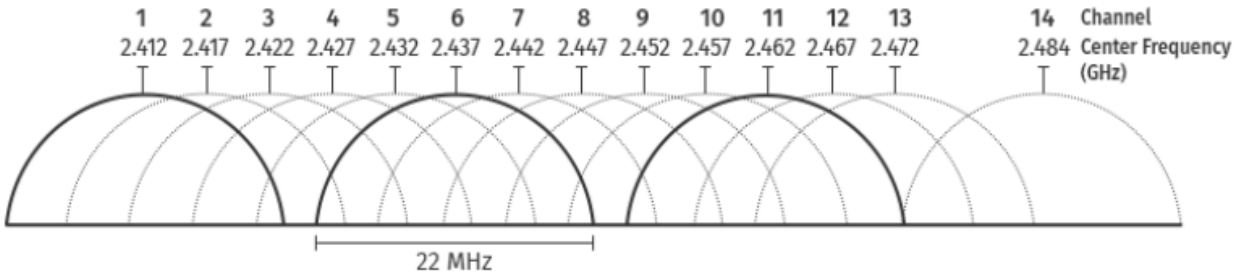

Рисунок 2.3 - Часткове перекриття бездротових каналів у діапазоні 2.4 ГГц [23, с.93].

Специфікації 802.11a, 802.11n і 802.11ac використовують більш жорстко регульований діапазон 5 ГГц, який пропонує до 165 каналів, що не перекриваються, з шириною каналу WiFi 20 МГц.

Ситуація в діапазоні 5 ГГц дещо ускладняється тим, що останні специфікації 802.11 дозволяють об'єднувати кілька каналів в групи для створення каналів шириною до 160 МГц.

Основна перевага цих широких каналів полягає в тому, що вони можуть передавати більше даних, але ця здатність має свою ціну, і ця ціна полягає в більш високому рівні шуму. Для каналів 20 МГц в діапазоні 5 ГГц цей рівень становить приблизно -101 дБм. Для каналів 160 МГц він становить -92 дБм.

Одним із способів протистояти підвищенню рівня фонової енергії є мінімізація відстані між точками доступу та клієнтськими пристроями. З надширокими каналами це часто неможливо без посилення самоперешкод, що робить менші розміри каналів кращим варіантом для багатьох розгортань Wi-Fi.

2.5 Висновки до другого розділу

Було проведено детальний аналіз та розроблено план дій з впровадження Wi-Fi мережі. Під час розробки структурної схеми Wi-Fi мережі було визначено необхідні компоненти та їх взаємозв'язок для забезпечення оптимального

функціонування мережі. Також було розроблено вимоги до проектування корпоративної бездротової мережі Wi-Fi.

Проведений аналіз потреб користувачів, технічні вимоги та можливості ринку сприяли обґрунтуванню вибору оптимального обладнання для реалізації Wi-Fi мережі. Враховуючи вимоги щодо швидкості, покриття та надійності зв'язку, були вибрані відповідні моделі точок доступу, комутаторів та іншого обладнання.

На основі характеристик обраного обладнання та аналізу потреб користувачів були розраховані зони покриття Wi-Fi сигналу. Це дозволило оптимізувати розташування точок доступу та забезпечити повне покриття необхідних зон з мінімальними зонами перекриття та слабкого сигналу.

Проведений розрахунок IP-адрес дозволив визначити необхідну кількість адрес для всіх пристроїв у мережі, включаючи точки доступу, комутатори, сервери та клієнтські пристрої. Це забезпечило належне функціонування мережі та уникнення конфліктів адрес. Планування та розгортання Wi-Fi мережі здійснене з врахуванням всіх необхідних аспектів та вимог, що дозволяє забезпечити високу якість зв'язку та задоволення потреб користувачів.

РОЗДІЛ 3. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕРЕЖІ WI-FI

Цей розділ присвячений аналізу та вдосконаленню методів захисту мережі Wi-Fi від різноманітних загроз, таких як несанкціонований доступ, перехоплення даних та вторгнення в мережевий трафік. Розглядаються різні аспекти забезпечення безпеки, включаючи, основні заходи безпеки при розгортанні мережі, а також розробку рекомендацій для підвищення рівня захищеності мережі Wi-Fi.

Мета цього розділу - надати читачам глибоке розуміння основних принципів та практичних методів забезпечення безпеки мережі Wi-Fi, щоб вони могли ефективно захищати свої мережі від потенційних загроз і забезпечувати безперебійний та безпечний доступ до інформації та ресурсів в Інтернеті.

3.1 Комплексні системи захисту інформації при розгортанні корпоративної мережі Wi-Fi

Комплексна система захисту інформації (КСЗІ) — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІКС [24].

КСЗІ включає заходи та засоби, що реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, який може здійснюватися шляхом підключення до обладнання та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів безпеки з метою використання інформації або нав'язування неправдивої інформації, використання вбудованих пристроїв або програм, використання комп'ютерних вірусів тощо. Необхідність забезпечення захисту інформації визначається насамперед вимогами нормативних документів.

При розгортанні корпоративної мережі Wi-Fi важливо вжити заходів для захисту інформації від несанкціонованого доступу, витоку та інших загроз. Для цього використовується комплексний підхід, який включає [25]:

1. Технічні заходи.

Використання сучасних протоколів шифрування, таких як WPA3-Enterprise з AES, є критично важливим для забезпечення безпеки Wi-Fi мережі. WPA3-Enterprise надає посилений захист даних порівняно з попередніми версіями протоколів, зокрема WPA2. Алгоритм AES (Advanced Encryption Standard) забезпечує високу стійкість до атак, роблячи майже неможливим перехоплення та розшифрування даних зловмисниками.

Аутентифікація користувачів є ключовим аспектом безпеки Wi-Fi мережі. Використання індивідуальних облікових даних для кожного користувача дозволяє контролювати доступ до мережі і відслідковувати активність кожного користувача. Це може бути реалізовано за допомогою протоколу IEEE 802.1X, який забезпечує централізовану аутентифікацію через сервер RADIUS (Remote Authentication Dial-In User Service). Такий підхід дозволяє підвищити рівень безпеки, оскільки кожен користувач має унікальний ідентифікатор і пароль, що унеможливлює несанкціонований доступ до мережі. Використовуйте сертифікат Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) на основі сертифікатів або краще, щоб захистити всю транзакцію автентифікації та комунікації.

Фільтрування трафіку є важливою складовою захисту мережі від несанкціонованого доступу і шкідливого контенту. Використання фаєрволу дозволяє забороняти доступ до певних веб-сайтів і ресурсів, які можуть становити загрозу для безпеки мережі. Це допомагає уникнути шкідливих атак, таких як фішинг та зараження вірусами.

MAC-фільтрація є додатковим заходом безпеки, який обмежує доступ до мережі лише для дозволених пристроїв на основі їх MAC-адрес. Хоча MAC-адреси можна підробити, цей метод є ефективним додатковим бар'єром проти небажаних підключень і зловмисників.

Вимкнення трансляції SSID (Service Set Identifier) є ще одним заходом безпеки, який може ускладнити доступ до мережі для сторонніх осіб. Якщо трансляцію SSID

вимкнено, точка доступу не рекламує своє існування, і до неї можуть підключатися лише ті користувачі, які знають цей параметр.

Сегментація мережі дозволяє підвищити рівень безпеки шляхом створення окремих підмереж для різних категорій користувачів та пристроїв. Наприклад, можна створити окремі Wi-Fi мережі для гостей, співробітників та пристроїв IoT (Internet of Things). Використання віртуальних LAN (VLAN) допомагає ізолювати підмережі одна від одної, що обмежує доступ до чутливої інформації і зменшує ризик витоку даних.

Встановлення системи виявлення вторгнень (IDS) та запобігання вторгненням (IPS) є важливими інструментами для захисту мережі від кібератак. IDS дозволяє виявляти підозрілу активність у мережі, аналізуючи трафік і порівнюючи його з відомими паттернами атак. IPS, в свою чергу, може не лише виявляти, але й блокувати такі атаки в режимі реального часу.

Регулярний моніторинг журналів бездротових точок доступу та контролерів дозволяє виявляти аномалії в діяльності мережі. Аналіз логів допомагає виявити незвичайну активність, таку як підозрілі підключення або спроби несанкціонованого доступу. Моніторинг журналів також допомагає в розслідуванні інцидентів безпеки і вдосконаленні політик безпеки.

Всі пристрої, підключені до мережі Wi-Fi, повинні бути захищені антивірусним і антималуерним програмним забезпеченням. Це забезпечує захист від шкідливих програм, вірусів та інших загроз, які можуть проникнути в мережу через вразливі пристрої.

2. Організаційні заходи.

Розробити та впровадити політику безпеки, яка регулює використання мережі Wi-Fi Перш за все, організація повинна створити детальну політику безпеки, яка регулює всі аспекти використання мережі Wi-Fi. Ця політика має охоплювати такі питання, як правила підключення до мережі, вимоги до паролів, протоколи безпеки, що використовуються для захисту даних, та обмеження на доступ до певних ресурсів.

Співробітники повинні бути навчені основам кібербезпеки та правилам використання мережі Wi-Fi. Навчання має бути регулярним, щоб постійно підтримувати високий рівень обізнаності серед працівників.

Контроль доступу. Слід обмежити доступ до адміністративних інтерфейсів мережевого обладнання лише авторизованим особам Для забезпечення безпеки мережі Wi-Fi важливо обмежити доступ до адміністративних інтерфейсів мережевого обладнання. Це можна досягти за допомогою багатофакторної аутентифікації, контролю доступу на основі ролей (RBAC).

Необхідно регулярно оновлювати програмне забезпечення мережевого обладнання, а також антивірусне та антималуерне програмне забезпечення, щоб закривати відомі вразливості та підвищувати захист від нових загроз.

3. Фізичні заходи.

Захист точки доступу Wi-Fi. Точка доступу Wi-Fi повинна бути встановлена в безпечному місці, недоступному для сторонніх осіб, щоб запобігти фізичному доступу до пристрою, що може призвести до його несанкціонованого переналаштування або навіть відключення.

Захист інформації від витоку технічними каналами (ТЗІ) є комплексом заходів, спрямованих на запобігання несанкціонованому доступу до інформації під час її обробки, передачі та зберігання. Технічні канали можуть включати в себе різноманітні методи отримання конфіденційної інформації, такі як перехоплення мережевого трафіку, використання підступів до мережевого обладнання та програмного забезпечення, а також експлуатація вразливостей систем.

3.2 Налаштування безпечної роботи пристроїв корпоративної бездротової мережі

Для захисту корпоративних бездротових мереж важливо вжити заходів для забезпечення безпечної роботи пристроїв, які до них підключаються. Цей підрозділ описує найкращі практики та рекомендації щодо налаштування пристроїв для безпечної роботи в корпоративній бездротовій мережі.

Рекомендовані налаштування Wi-Fi роутера ASUS RT-AC5300 для забезпечення безпечної роботи в корпоративній бездротовій мережі [26]:

1.1 Зміна пароля адміністратора:

- перейдіть до веб-інтерфейсу роутера за адресою 192.168.1.1.;
- введіть ім'я користувача та пароль за замовчуванням (зазвичай admin/admin);
- перейдіть до розділу "Адміністрування" -> "Системні параметри" -> "Пароль адміністратора";
- введіть старий пароль, а потім введіть та підтвердіть новий.

1.2 Налаштування бездротової мережі.

Створіть два окремі точки доступу одна для корпоративної мережі, а друга для гостей.

Для корпоративної мережі:

1. Виберіть WPA3-Enterprise як тип аутентифікації;
2. Виберіть AES як тип шифрування;
3. Введіть RADIUS-сервер та секретний ключ з’єднання;
4. Вимкніть SSID Broadcast. Якщо цю функцію увімкнено, для доступу до бездротової мережі потрібно буде ввести SSID вручну на бездротовому пристрої.

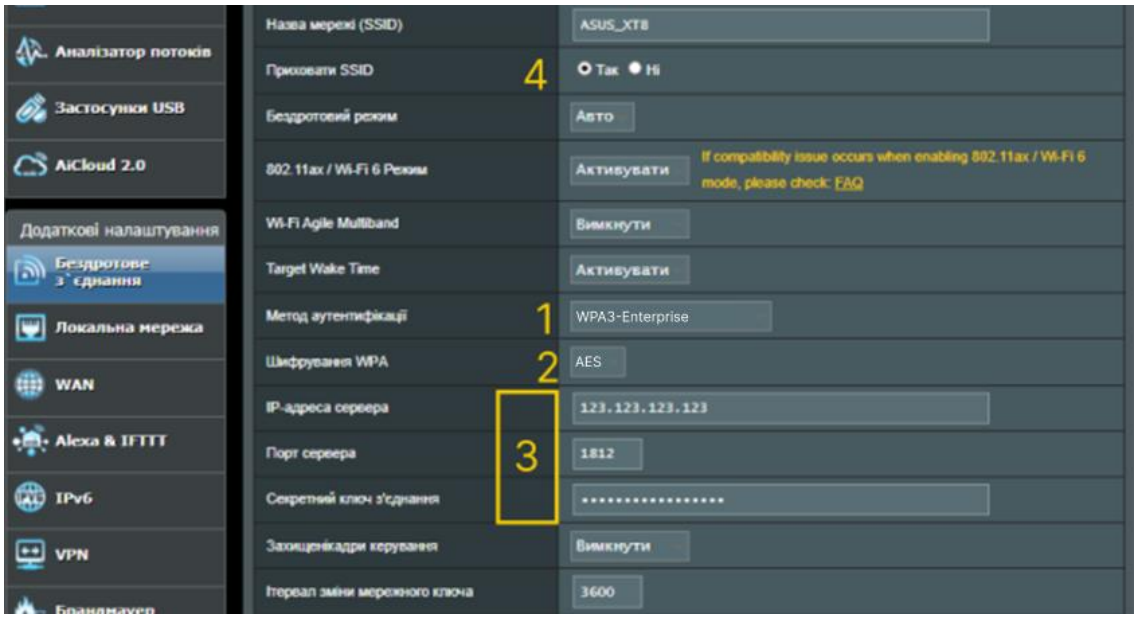

Рисунок 3.2 - Налаштування бездротової мережі

Для гостьовьової мережі:

1. На навігаційній панелі перейдіть до Загальне > Гостьова мережа.

2. На екрані Гостьова мережа виберіть діапазон частот 2,4 ГГц або 5 ГГц для гостьової мережі, яку ви хочете створити.

3. Натисніть Увімкнути.

4. Виберіть Метод автентифікації.

5. Якщо ви вибрали метод автентифікації WPA, виберіть Шифрування WPA.

6. Вкажіть Час доступу або виберіть Безлімітний.

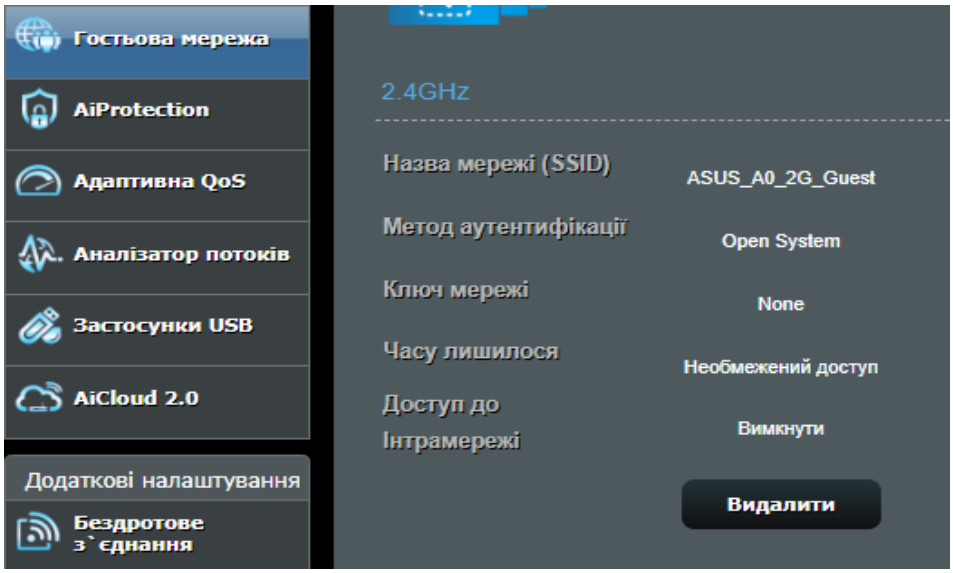

Рисунок 3.3 – Впровадження гостьової мережі

1.3 Створення віртуальної локальної мережі (VLAN).

VPN забезпечує безпечне з'єднання з віддаленим комп'ютером або віддаленою мережею, використовуючи загальнодоступну мережу, таку як Інтернет.

Налаштування доступу до VPN-сервера:

1. На навігаційній панелі перейдіть до Розширені налаштування > VPN сервер.

2. У полі Увімкнути VPN-сервер натисніть Так.

3. У випадаючому списку Деталі VPN виберіть Розширені налаштування, якщо хочете налаштувати розширені параметри VPN, такі як підтримка широкомовлення, автентифікація, шифрування MPPE та діапазон клієнтських IP-адрес.

4. У полі Підтримка Network Place (Samba) виберіть Так.

5. Введіть ім'я користувача та пароль для доступу до VPN-сервера. Натисніть кнопку +.

6. Натисніть кнопку Застосувати.

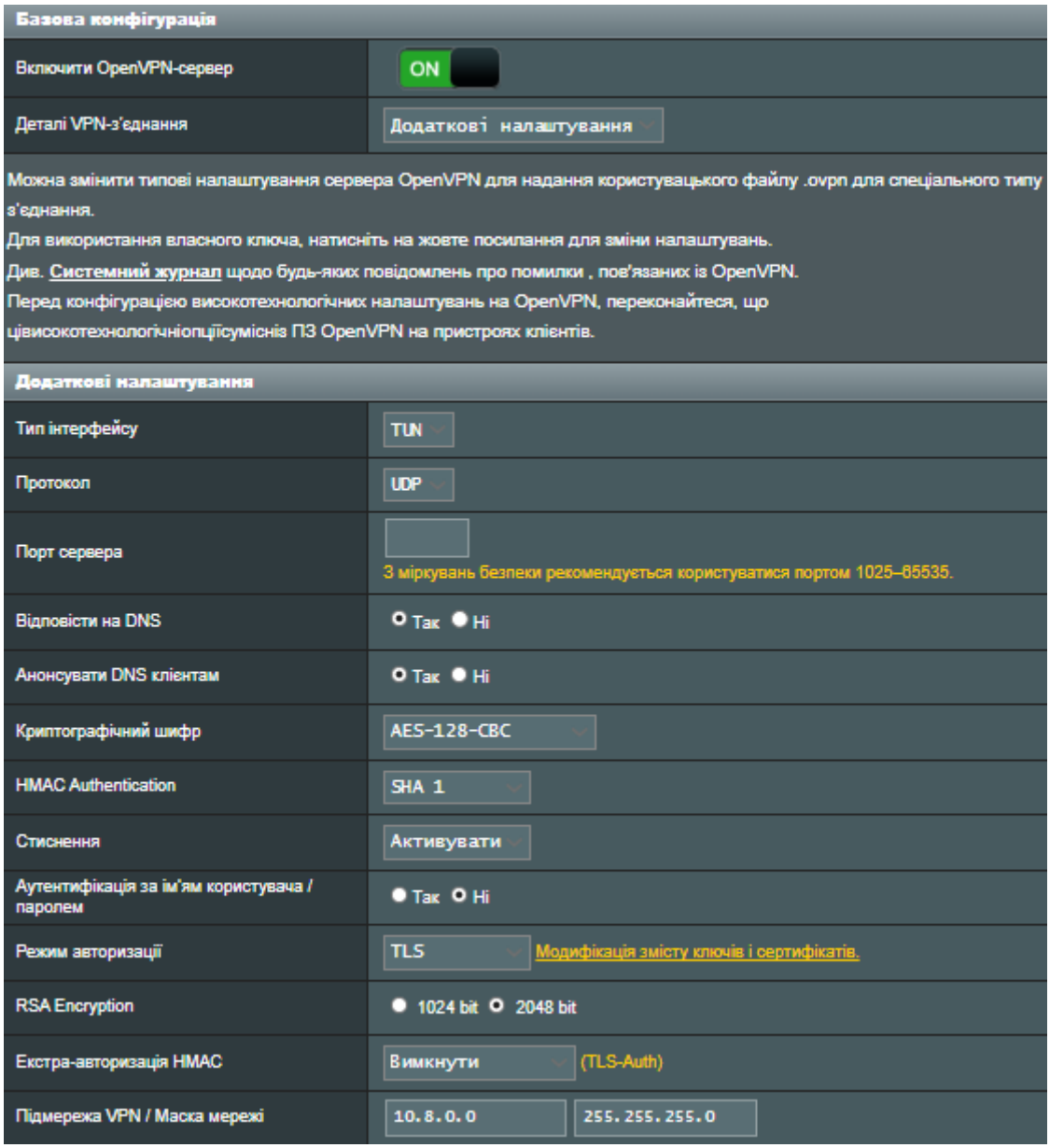

Рисунок 3.4 – Налаштування VLAN

1.4 Увімкніть брандмауер на роутері. Для цього потрібно:

1. Перейти до розділу "Безпека" -> "Брандмауер".

2. Створити правило брандмауера, яке дозволяє доступ до корпоративної мережі лише для дозволених IP-адрес.

1.5 Увімкніть фільтрацію MAC-адрес.

Бездротовий MAC-фільтр забезпечує контроль над пакетами, що передаються на вказану MAC-адресу (Media Access Control) у вашій бездротовій мережі.

Ця функція дозволяє вручну обмежити коло пристроїв, які можуть підключатися до мережі Wi-Fi. Фільтрація відбувається на основі унікальних ідентифікаторів мережевих карт клієнтів — MAC-адрес, які додаються до списку дозволених. Пристрої, що не входять до цього списку, не зможуть підключитися, навіть якщо знають ключ шифрування WPA3. Проте, цей захист можна обійти, змінивши MAC-адресу свого мережевого адаптера за допомогою відповідного програмного забезпечення. Однак, незважаючи на це, бажано використовувати цей вид захисту для підвищення загальної безпеки системи зв’язку.

Щоб налаштувати фільтр MAC-адрес бездротових мереж:

1. На навігаційній панелі перейдіть до Розширені налаштування > Бездротовий зв'язок > вкладка Фільтр MAC-адрес бездротових мереж.

2. Установіть галочку Так у полі Увімкнути фільтр Mac-адрес.

3. У розкривному списку Режим фільтрації MAC-адрес виберіть Прийняти або Відхилити.

Виберіть Прийняти, щоб дозволити пристроям зі списку фільтра MAC-адрес доступ до бездротової мережі.

Виберіть Відхилити, щоб заборонити пристроям зі списку фільтра MAC-адрес доступ до бездротової мережі.

4. У списку фільтрів MAC-адрес натисніть кнопку Додати і введіть MAC-адресу бездротового пристрою.

5. Натисніть Застосувати.

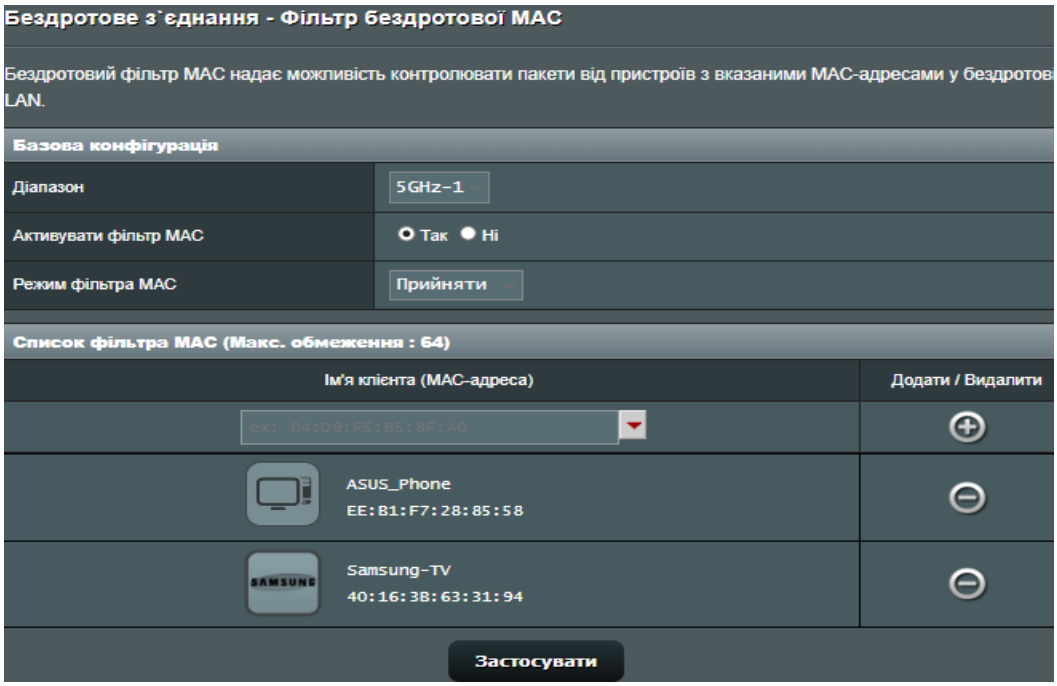

Рисунок 3.5 – Встановлення фільтрації MAC-адрес

1.6 Вимкніть SSH, що не дозволить проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань.

1.7 Вимкніть UPnP. Це протокол, який звільняє вас від ручного налаштування мережі та дає змогу під'єднувати пристрої до вашої мережі. У разі ввімкненого UPnP пристрої безпосередньо переспрямовують порт на вашому маршрутизаторі та позбавляють вас необхідності переадресації портів вручну.

Встановлення моніторингу мережі та системи виявлення та запобігання вторгнень.

В даній корпоративній мережі раціонально буде використовувати хмарну систему SIEM. Система пропонує всі можливості традиційної SIEM, але розміщене в хмарі. Вона збирає, аналізує та управляє даними про безпеку з різних джерел по всій інфраструктурі організації, щоб забезпечити розуміння подій та загроз безпеки в режимі реального часу. Такий варіант забезпечує функціональність SIEM зі значно меншими витратами на розгортання.

Налаштування системи виявлення та запобігання вторгненням є одним із ключових заходів для захисту бездротової корпоративної мережі від можливих нападів. Щоб налаштувати IDS/IPS, необхідно виконати такі дії:

1. Налаштуйте віддзеркалення портів на комутаторах таким чином, щоб вони надсилали копію всього трафіку на IDS/IPS.

2. Впровадити безпечні інтерфейси між мережевими пристроями та IDS/IPS для безпечних з’єднань.

3. Встановіть правила в системі IDS/IPS, які можуть виявляти будь-яку ненормальну активність, яка може вказувати на відому сигнатуру атаки.

4. Крім того, переконайтеся, що існують правила, налаштовані таким чином, щоб вони могли автоматично блокувати або обмежувати будь-які підозрілі підключення, виявлені системою.

Базу даних підписів слід регулярно оновлювати, щоб правила залишалися актуальними.

Налаштування брандмауера для корпоративної мережі.

Брандмауер діє як бар'єр безпеки між вашою надійною внутрішньою мережею та Інтернетом. Для введення пристрою в роботу необхідно зробити наступні кроки.

Крок перший - почніть з початкового налаштування. Для цього вам потрібно отримати доступ до веб-інтерфейсу або консолі брандмауера. Під час початкової конфігурації ви зазвичай налаштовуєте основні параметри, такі як мережеві інтерфейси, IP-адреси та адміністративні паролі.

По-друге, установіть різні зони мережі в межах брандмауера. Вони можуть включати довірену зону для користувачів вашої внутрішньої мережі, ненадійну зону, що представляє підключення до Інтернету, і, можливо, зону DMZ, на якій розміщені загальнодоступні сервери.

Наступним кроком є створення правил брандмауера для керування вхідним і вихідним мережевим трафіком: дозвольте авторизований трафік (наприклад, перегляд веб-сторінок або електронну пошту), одночасно забороняючи сумнівні або неавторизовані підключення.

Нарешті, забезпечте належну реєстрацію та моніторинг. Увімкніть функцію журналювання, щоб відстежувати дії брандмауера, що може допомогти в майбутніх перевірках або усуненні несправностей. Налаштуйте можливості моніторингу, які б виявляли аномальну поведінку трафіку, таким чином натякаючи на будь-які виявлені інциденти безпеки.

Налаштування автентифікації користувачів за стандартом IEEE 802.1X з допомогою сервера RADIUS [27].

1. Налаштування сервера RADIUS:

- відредагуйте конфігураційні файли RADIUS (наприклад, `radiusd.conf` для FreeRADIUS) для налаштування клієнтів (точок доступу або комутаторів) і політик автентифікації;
- додайте інформацію про клієнтів у файлі `clients.conf`, вказавши IP-адресу точки доступу або комутатора та спільний секрет;
- налаштуйте політики автентифікації у файлі `users` або налаштуйте інтеграцію з Active Directory/LDAP для динамічної автентифікації користувачів.

2. Налаштування точки доступу або комутатора:

- увійдіть в інтерфейс управління точкою доступу або комутатором;
- перейдіть до розділу налаштування безпеки (звичайно "Security" або "Authentication");
- активуйте IEEE 802.1X автентифікацію;
- вкажіть IP-адресу сервера RADIUS, порт (зазвичай 1812 для автентифікації), та спільний секрет, що збігається з налаштуванням на сервері RADIUS.

3. Налаштування клієнтських пристроїв:

- на кожному клієнтському пристрої налаштуйте підключення до Wi-Fi мережі з використанням 802.1X автентифікації;
- вкажіть тип автентифікації, зазвичай EAP (наприклад PEAP, EAP-TLS);
- введіть облікові дані, які відповідають даним в системі автентифікації (наприклад, ім'я користувача та пароль Active Directory).

Налаштування автентифікації за стандартом IEEE 802.1X з використанням сервера RADIUS забезпечує високий рівень безпеки для корпоративної бездротової мережі, запобігаючи несанкціонованому доступу та забезпечуючи централізоване управління автентифікацією користувачів.

Налаштування кінцевих пристроїв.

Кінцеві точки, такі як комп'ютери, ноутбуки та мобільні пристрої, необхідні для щоденної роботи, але також можуть бути точками входу для порушень безпеки. Тому важливо подбати про їх правильне впровадження в систему.

Підготовка:

1. Підтримуйте оновлений список усіх пристроїв, що мають доступ до мережі. Розробіть політику використання власних пристроїв (BYOD), що визначає прийнятні правила використання та протоколи безпеки для персональних пристроїв.

2. Запровадьте політику своєчасного оновлення операційних систем і додатків на всіх кінцевих точках. Ці оновлення часто включають патчі безпеки для усунення вразливостей.

3. Впровадьте політику надійних паролів та забезпечте багатофакторну автентифікацію (MFA) для всіх облікових записів користувачів.

Конфігурація:

1. Встановіть і налаштуйте надійне антивірусне та антивірусне програмне забезпечення для виявлення та запобігання загрозам.

2. Розгляньте можливість впровадження білих списків додатків, які обмежують роботу кінцевих точок лише дозволеними програмами, зменшуючи ризик виконання шкідливого програмного забезпечення.

3. Якщо віддалений доступ необхідний, налаштуйте безпечні протоколи віддаленого доступу та обмежте доступ лише для авторизованого персоналу та пристроїв.

4. Увімкніть шифрування дисків на всіх кінцевих точках, щоб захистити конфіденційні дані навіть у разі втрати або крадіжки пристрою.

Додаткові міркування:

- впроваджуйте заходи фізичної безпеки для запобігання несанкціонованому доступу до пристроїв, наприклад, вимагайте входу в систему після періодів бездіяльності;
- встановіть політику використання зовнішніх накопичувачів щоб мінімізувати ризик впровадження шкідливого програмного забезпечення;
- регулярно проводьте сканування вразливостей на кінцевих точках для виявлення та усунення потенційних вразливостей безпеки.

3.3 Розробка політики інформаційної безпеки в корпоративній бездротовій мережі

В умовах постійних кібератак, витоку конфіденційної інформації та інших загроз, необхідно розробляти ефективні стратегії забезпечення безпеки корпоративних мереж.

Політика інформаційної безпеки поєднує в собі правила, норми та процедури, яких необхідно дотримуватись, у чіткому та стислому документі. Вона діє як ресурс для працівників, описуючи, як ваша організація зберігає, захищає та поширює інформацію, а також очікування від працівників.

Оскільки організації мають різні бізнес-вимоги, зобов'язання щодо дотримання нормативних вимог та штатний розклад, не існує єдиної політики інформаційної безпеки, яка б працювала для всіх. Натомість кожен IT-відділ повинен визначити, які саме варіанти політики найкраще відповідають його конкретним потребам, і створити чіткий документ, який буде схвалений зацікавленими сторонами на високому рівні.

Реалізація ефективної політики реагування на інцидент може допомогти захистити вашу корпоративну мережу від кіберінцидентів та зменшити їх наслідки.

Нижче наведено перелік важливих аспектів, які слід враховувати при розробці політики інформаційної безпеки [28]:

1. Мета. Загальною метою політики інформаційної безпеки є захист інформаційних активів організації від різноманітних загроз. Конкретні цілі політики інформаційної безпеки можуть варіюватися залежно від потреб та особливостей організації.

2. Аудиторія. Визначте аудиторію, на яку поширюється політика інформаційної безпеки. Також можна вказати, які аудиторії не підпадають під сферу дії політики (наприклад, співробітники іншого підрозділу, який керує безпекою окремо, можуть не підпадати під сферу дії політики).

3. Класифікація даних. Політика повинна класифікувати дані за категоріями, які можуть включати "цілком таємно", "таємно", "конфіденційно" та "публічно". Цілі класифікації даних такі:

- зрозуміти, які системи, операції та додатки стосуються найбільш чутливих та контрольованих даних, щоб належним чином розробити засоби контролю безпеки для цього обладнання та програмного забезпечення;
- забезпечити неможливість доступу до конфіденційних даних особам з низьким рівнем допуску;
- захистити дуже важливі дані та уникнути непотрібних заходів безпеки для неважливих даних.

4. Обізнаність та поведінка щодо безпеки.

Поділіться політикою IT-безпеки зі своїм персоналом. Проводьте тренінги для інформування працівників про ваші процедури та механізми безпеки, включаючи заходи захисту даних, заходи захисту доступу та класифікацію конфіденційних даних.

Зробіть особливий акцент на небезпеці атак соціальної інженерії (наприклад, фішингових електронних листів або інформаційних запитів через телефонні дзвінки). Покладіть на всіх співробітників відповідальність за виявлення, запобігання та повідомлення про такі атаки.

Політика чистоти на робочому столі. Подрібнюйте конфіденційні документи, які більше не потрібні. Тримайте принтери в чистоті, щоб документи не потрапляли до чужих рук.

Попрацюйте з відділом кадрів, щоб визначити, як слід обмежити доступ до Інтернету як на робочих місцях, так і для віддалених співробітників, які використовують ресурси організації. Блокуйте небажані веб-сайти за допомогою проксі-сервера.

5. Політика шифрування.

Шифрування передбачає кодування даних, щоб зробити їх недоступними або прихованими від сторонніх осіб. Це допомагає захистити дані, що зберігаються в стані спокою та під час переміщення між локаціями, а також гарантує, що конфіденційні, приватні та службові дані залишаться приватними. Це також може підвищити безпеку комунікації між клієнтом і сервером. Політика шифрування допомагає організаціям визначити:

- пристрої та носії, які організація повинна шифрувати;
- коли шифрування є обов'язковим;
- мінімальні стандарти, що застосовуються до обраного програмного забезпечення для шифрування.

6. Політика резервного копіювання даних.

Політика резервного копіювання даних визначає правила та процедури створення резервних копій даних. Вона є невід'ємним компонентом загальної стратегії захисту даних, безперервності бізнесу та аварійного відновлення. Основні функції політики резервного копіювання даних:

- визначає всю інформацію, яку організація повинна створювати резервні копії;
- визначає частоту резервного копіювання, наприклад, коли виконувати первинне повне резервне копіювання, а коли - інкрементні резервні копії;
- визначає місце зберігання резервних копій даних;

- перераховує всі ролі, відповідальні за процеси резервного копіювання, наприклад, адміністратор резервного копіювання та члени IT-команди.

7. Відповідальність, права та обов'язки персоналу. Призначте персонал для проведення перевірок доступу користувачів, навчання, управління змінами, управління інцидентами, впровадження та періодичного оновлення політики безпеки. Обов'язки повинні бути чітко визначені як частина політики безпеки.

8. Критерії зміцнення системи. Політика інформаційної безпеки повинна містити посилання на контрольні показники безпеки, які організація буде використовувати для зміцнення критично важливих систем.

9. Модель загроз/порушника та їх рівень. Моделі загроз/порушників використовуються для оцінки ризиків, пов'язаних з інформаційною безпекою. Вони допомагають визначити ймовірні типи загроз, які можуть виникнути, а також потенційних порушників, які можуть їх здійснити.

Рівні загроз поділяються на:

1. Низький рівень загрози:

- мотиви: випадкові або мінімально мотивовані дії;
- засоби: прості методи, такі як фішинг, соціальна інженерія;
- знання та навички: мінімальні технічні знання;
- цілі: здебільшого випадкові або ненавмисні атаки.

2. Середній рівень загрози:

- мотиви: фінансова вигода, конкурентна розвідка;
- засоби: використання спеціалізованих інструментів, але з обмеженими ресурсами;
- знання та навички: середній рівень технічних знань;
- цілі: отримання доступу до конфіденційної інформації, порушення роботи систем.

3. Високий рівень загрози:

- мотиви: стратегічні або політичні цілі;
- засоби: використання передових методів та інструментів, значні ресурси;

- знання та навички: високий рівень технічних знань та досвіду;
- цілі: кібершпигунство, кібервійна, серйозні порушення діяльності системи.

10. Політика реагування на кіберінцидент в корпоративній мережі.

Політика реагування на кіберінцидент - це документ, який описує дії, які повинні бути вжиті у разі виявлення кіберінциденту в корпоративній мережі.

Політика реагування на інцидент повинна включати наступні розділи:

- визначення інциденту: що таке кіберінцидент і які його ознаки;
- протокол реагування: хто відповідає за реагування на інцидент і що їм робити;
- процес розслідування: як розслідувати інцидент і визначити його причину;
- ліквідація наслідків: як ліквідувати наслідки інциденту;
- відновлення: як відновити нормальну роботу мережі та систем;
- звітування: як звітувати про інцидент;
- профілактика: як запобігти повторенню подібних інцидентів;

Важливо регулярно оновлювати та переглядати політику та процедури інформаційної безпеки, щоб гарантувати, що вони відповідають потребам вашої організації.

3.4 Висновки до третього розділу

Застосування комплексних систем захисту інформації є критично важливим для забезпечення безпеки мережі Wi-Fi. Ці системи включають в себе комбінацію апаратних та програмних засобів, таких як брандмауери, антивіруси, системи виявлення вторгнень та інші, які спільно працюють для захисту мережі від різних загроз.

Налаштування безпечної роботи пристроїв у корпоративній бездротовій мережі включає в себе ряд заходів, таких як встановлення складних паролів,

використання методів шифрування, обмеження доступу до мережевих ресурсів лише авторизованим користувачам та регулярне оновлення програмного забезпечення.

Розробка політики інформаційної безпеки в корпоративній бездротовій мережі є важливою складовою заходів забезпечення безпеки. Ця політика повинна включати в себе визначення правил щодо використання мережі, заходи з контролю доступу, процедури реагування на інциденти безпеки та відповідальність за порушення цих правил.

Забезпечення інформаційної безпеки мережі Wi-Fi вимагає комплексного підходу, який включає в себе технічні, організаційні та процедурні заходи для ефективного захисту від різноманітних загроз.

ВИСНОВКИ

У цій кваліфікаційній роботі було проведено дослідження можливостей технології Wi-Fi для побудови корпоративної локальної мережі, а також проблем інформаційної безпеки, пов'язаних з її використанням. Були проаналізовані різні підходи до вирішення цих проблем, а також розроблені рекомендації щодо забезпечення інформаційної безпеки корпоративної локальної мережі на основі Wi-Fi.

В ході виконання роботи були отримані наступні важливі наукові та практичні результати:

1. Проведено аналіз можливостей технології бездротового зв'язку Wi-Fi для побудови корпоративних локальних мереж. Визначено поняття та принцип роботи Wi-Fi, а також розглянуто стандарти мереж Wi-Fi, що дозволило зрозуміти та врахувати особливості цієї технології при плануванні та розгортанні мережі.

2. Розглянуто можливі типи атак на бездротову мережу та заходи для їх запобігання. Бездротові мережі вразливі до різних типів атак, таких як перехоплення даних (eavesdropping), атаки "людина посередині" (MITM), підробка (spoofing), атаки на доступність (DoS/DDoS) і експлуатація слабких паролів. Запобігти цим атакам можна за допомогою шифрування даних (WPA3), використання сильних паролів і регулярної їх зміни, фільтрації MAC-адрес, а також моніторингу мережі для виявлення аномальної активності.

3. Розроблено планування та розгортання мережі на базі технології Wi-Fi, що включає в себе розробку структурної схеми мережі, вибір обладнання, розрахунок зон покриття та розрахунок IP-адрес та планування каналів, що сприяє ефективному функціонуванню мережі.

4. Комплексний підхід до забезпечення інформаційної безпеки мережі Wi-Fi дозволяє ефективно захищати конфіденційні дані та запобігати несанкціонованому доступу до мережевих ресурсів.

5. Вивчено та розроблено заходи забезпечення інформаційної безпеки мережі Wi-Fi, зокрема налаштування безпечної роботи пристроїв корпоративної бездротової мережі та розробку політики інформаційної безпеки в корпоративній бездротовій мережі.

Результати дослідження можуть бути використані для розробки та впровадження безпечних та надійних корпоративних мереж Wi-Fi, що відповідають сучасним вимогам інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Jordi Salazar. Wireless networks 1st Edition, 2017 – 37c.
2. James F. Kurose, Keith W. Ross. Computer networking : a top-down approach —6th ed., 2013. – 862c.
3. Matthew Gast. 802.11 Wireless Networks:The Definitive Guide, 2002 – 464 с.
4. IEEE SA - The Evolution of Wi-Fi Technology and Standards [Електронний ресурс] - Режим доступу: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/
5. Jennifer Minella. Wireless Security Architecture: Designing and Maintaining Secure Wireless for Enterprise, 2022. – 584 с.
6. Jonathan Hassell. RADIUS 1st Edition, 2002. – 190c.
7. Emmett Dulaney. Network+ N10-008 Exam Cram, 2022. – 756c.
8. Doug Lowe. Networking All-in-One Desk Reference For Dummies: 8th Edition, 2021 - 1056c.
9. Kanawat Sachin, Parihar Pankaj. Attacks in Wireless Networks. International Journal of Smart Sensor and Ad-Hoc Networks, 2011. - 116c.
10. Lawrie Brown, William Stallings. Computer security : principles and practice — Third edition, 2014. – 838c.
11. Asmaa Halbouni. Wireless Security Protocols WPA3: A Systematic Literature Review, 2023. – 13c.
12. Alberto Bartoli. Understanding Server Authentication in WPA3 Enterprise, 2020. - 12c.
13. В. Л. Бурячок. Технології забезпечення безпеки мережевої інфраструктури / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
14. Nigel Chapman, Jenny Chapman. Authentication and Authorization on the Web, 2012. – 233c.

15. Jon C. Snader. VPNs Illustrated Tunnels, VPNs, and Ipsec, 2006. – 481с.

16. Karen Scarfone. Guide to Intrusion Detection and Prevention Systems (IDPS), 2012. – 111с.

17. Технології захисту інформації в інформаційно-телекомунікаційних системах / А. В. Жилін; КПІ ім. Ігоря Сікорського, Київ 2021. – 213 с.

18. UniFi [Електронний ресурс] - Режим доступу: https://store.ui.com/us/en/collections/unifi-wifi-flagship-high-capacity/products/u6-pro

19. ASUS RT-AX88U Pro [Електронний ресурс] - Режим доступу: https://www.asus.com/networking-iot-servers/wifi-routers/asus-gaming-routers/rt-ax88u-pro/

20. TP-Link [Електронний ресурс] - Режим доступу: https://www.tp-link.com/uk-ua/business-networking/poe-switch/tl-sg3210xhp-m25

21. Модель загроз безпеки у бездротових системах зв’язку міліметрового діапазону хвиль. / Д.С. Сальников, О. І. Цопа, 2018. – 10с.

22. Mahdi Saleh. Internet Protocol (IP) Addressing, 2017. – 94с.

23. Ilya Grigorik. High Performance Browser Networking, 2013. – 400с.

24. Поради (рекомендації) щодо створення КСЗІ в ІКС, які використовуються для надання послуг доступу до мережі Інтернет [Електронний ресурс] - Режим доступу: https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet

25. Joseph F. Matthews. A Secure Approach to Deploying Wireless Networks, 2016. - 21с.

26. User Guide RT-AC5300 Wireless-AC5300 Tri-band Gigabit Router, First Edition, 2015. – 142с.

27. THE FREERADIUS TECHNICAL GUIDE, Network RADIUS SARL, 20 – 158с.

28. ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements – 30с.

UNICHECK
by Turnitin

Ім'я користувача:
Комп'ютерної математики та інформаційної безпеки...

ID перевірки:
1016349879

Дата перевірки:
11.06.2024 23:59:59 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
12.06.2024 00:05:54 EEST

ID користувача:
100005746

Назва документа: Диплом Кулаковська А.С

Кількість сторінок: 67 Кількість слів: 13284 Кількість символів: 101161 Розмір файлу: 948.66 KB ID файлу: 1016153257

4.5%
Схожість

Найбільша схожість: 0.51% з Інтернет-джерелом (https://ela.kpi.ua/handle/123456789/43198)

2.71% Джерела з Інтернету	149	Сторінка 69
3.7% Джерела з Бібліотеки	167	Сторінка 70

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	6