Міністерство освіти і науки України
Сумський державний університет
Кафедра електроніки і комп’ютерної техніки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проєкту

на тему:

«Проєктування телекомунікаційної мережі підприємства на базі стандартів IEEE 802»

Завідуючий кафедри А. С. Опанасюк

Керівник проєкту О. В. Д’яченко

Студент групи ТК-71 В. М. Коник

Суми 2021

Сумський державний університет

Факультет денний **Кафедра** електроніки і комп'ютерної техніки

Спеціальність Телекомунікації та радіотехніка

ЗАТВЕРДЖУЮ**:**
Зав. кафедри ЕКТ
Опанасюк А. С.
«___» _____ 2021 р.

Завдання

на дипломний проєкт студенту

Коник Валерія Миколаївна
(прізвище,ім'я,по батькові)

1. Тема проєкту: Проєктування телекомунікаційної мережі підприємства на базі стандартів IEEE 802
затверджено наказом університету від «05» травня 2021 р. № 0154-VI

2. Термін здачі студентом закінченого проєкту 2 червень 2021 р.

3. Вихідні дані до проєкту: Розрахувати параметри мережі підприємства на основі стандартів IEEE 802.11. Рішення повинно працювати на двох діапазонах 2.4 і 5 ГГц. Забезпечити стабільне покриття мережі приміщення підприємства.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які підлягають розробці)

Огляд літературних джерел по тематиці проєкту. Розрахунки покриття оптимальної зони бездротової мережі для приміщення підприємства.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проєкту	Термін виконання етапів проєкту	Примітка
1.	Огляд літератури по тематиці проєкту	15.04.21	
2.	Написання першого розділу	25.04.21	
3.	Написання другого розділу	29.04.21	
4.	Написання третього розділу	10.04.21	
5.	Коригування дипломного проекту	16.05.21	
6.	Оформлення графічної частини	20.05.21	
7.	Оформлення пояснювальної записки	30.05.21	
8.	Рецензування роботи та підготовка до захисту	07.06.21	

Студент-дипломник _____
(підпис)

Керівник проєкту _____
(підпис)

РЕФЕРАТ

Робота містить 45 сторінок, 13 рисунків, 8 таблиці.

У даному дипломному проекті розглянуто план побудови мережі бездротового Wi-Fi зв'язку на основі стандарту (IEEE-802) підприємства. У роботі представлені характеристики стандарту, відмінність його від інших стандартів, схема побудови мережі та склад обладнання.

Ключові слова: Wi-fi, 802.11, роутер, характеристики, інформація, шифрування, розрахунок, планування, мережа.

Keywords: Wi-fi, 802.11, router, characteristics, information, encryption, calculation, planning, network.

ЗМІСТ

ВСТУП 4
1 ОГЛЯД ТЕХНОЛОГІЇ БЕЗДРОТОВОГО ДОСТУПУ Wi-FI 5
1.1 розвитку технологій бездротового доступу 5
1.2 Стандарти бездротового зв'язку IEEE 802 7
1.3 Режими роботи бездротових мереж Wi-Fi 14
2 РЕАЛІЗАЦІЯ МЕРЕЖІ БЕСПРВОДНОГО ДОСТУПУ 21
2.1 Місце реалізації проекту 21
2.2 Вибір обладнання 22
2.2.1 Роутер Xiaomi Mi WiFi Router 4A 22
2.2.2 Бездротовий роутер Xiaomi Redmi AX5 26
2.2.3 Маршрутизатор Xiaomi AIoT Router AX3600 28
2.3. Розрахунок дальності роботи бездротового каналу зв'язку 802.11 31
3. Стандарти безпеки 35
3.1 WPA 35
3.2 WPA2 36
3.3 WPA3 37
3.3.1 Основні відомості 37
3.3.2 Слабкий пароль 39
3.3.3 Відсутність прямої секретності 39
3.3.4 Підміна і розшифровка пакетів WPA 40
3.3.5 Відновлення PIN-коду WPS 41
3.3.6 MS-CHAPv2 і відсутність перевірки CN сервера AAA 41
3.3.7 Прогнозований Груповий часовий ключ (GTK) 42
3.3.8 Атака KRACK 43
ВИСНОВКИ 44
СПИСОК ЛІТЕРАТУРИ 45
ДОДАТОК 1 3

					ЕлІТ 6.172.366 ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Коник В.М.			Проєктування телекомунікаційної мережі підприємства на базі стандартів IEEE 802	Літ.	Арк. 3 / Аркушів 45
Перевір.		Д'яченко О. В.					
Затвердж.		Опанасюк А.С.				СумДУ, ТК-71	

ВСТУП

У всьому світі стрімко зростає потреба в бездротових з'єднаннях, особливо в сфері бізнесу та IT технологій. Користувачі з бездротовим доступом до інформації завжди і скрізь можуть працювати набагато більш продуктивно і ефективно, ніж їх колеги, прив'язані до дротових телефонних і комп'ютерних мереж, так як існує прихильність до певної інфраструктури комунікацій.

На сучасному етапі розвитку мережевих технологій, Технологія бездротових мереж Wi-Fi є найбільш зручною в умовах вимагають мобільність, простоту установки і використання. Wi-Fi (від англ. wireless fidelity-бездротовий зв'язок)-стандарт широкосмугового бездротового зв'язку сімейства 802.11 розроблений в 1997р. як правило, технологія Wi-Fi використовується для організації бездротових локальних комп'ютерних мереж, а також створення так званих гарячих точок високошвидкісного доступу в інтернет.

Бездротові мережі мають, в порівнянні з традиційними дротовими мережами, чималими перевагами, головним з яких, звичайно ж, є:

- Простота розгортання та гнучкість архітектури мережі;
- Швидкість проектування та реалізації;
- Бездротова мережа не потребує прокладання кабелів .

Також вона має свої недоліки такі як швидкість з'єднання і радіусу дії і наявності перешкод навідстоні між приймачем і передавачем.

Метою даної роботи є проектування мережі бездротового доступу на підприємстві, з метою підвищення рівня інформатизації, надання сучасних послуг зв'язку: високошвидкісний доступ в інтернет, комп'ютерна мережа, на базі технології Wi-Fi.

1 ОГЛЯД ТЕХНОЛОГІЇ БЕЗДРОТОВОГО ДОСТУПУ Wi-FI

1.1 розвитку технологій бездротового доступу

Wi-Fi залишається однією з найбільш перспективних технологій бездротового зв'язку і вона стрімко розвивається і приймає в себе нові бездротові рішення, що дозволяють збільшити швидкість передачі даних. Навіть з розвитком LTE-мереж, Wi-Fi не залишається осторонь, а швидше отримує додаткову гілку розвитку, розвантажуючи трафік в найбільш затребуваних ділянках мережі.

Wi-Fi для застосування всередині приміщень в рамках встановленої законодавством потужності випромінювання не вимагає отримання дозволу на використання частот. Крім того, організація Wi-Fi-мережі в умовах будинку або невеликого офісу досить проста. Проте, при проектуванні мережі з високими вимогами до якості зв'язку, щільності покриття і пропускної здатності, як правило, вдаються до допомоги фахівців. Розгортання Wi-Fi-мережі займає на порядок менше часу в порівнянні з прокладкою СКС до робочих місць. Саме за простоту Налаштування, розгортання, відносну дешевизну і зручність, Wi-Fi по праву вважають однією з перспективних і активно розвиваються технологій.

Вимоги до Wi-Fi-обладнання описані в наборі стандартів IEEE 802.11. З випуском кожного нового стандарту, до 802.11 додавалася буква, наприклад, 802.11 a/b / n і т.д. на сьогоднішній день налічується кілька десятків різновидів стандартів Wi-Fi. Не всі стандарти були спрямовані на збільшення швидкості передачі даних, деякі з них зачіпають питання безпеки (наприклад, 802.11 i), інші включали опис роботи роумінгу (802.11 r) і т. д.

У таблиці нижче наведені стандарти бездротового зв'язку Wi-Fi, в яких проводилося збільшення швидкостей передачі даних:

Таблиця 1.1 – Стандарти

Стандарт	Діапазон	Рік виходу	Орієнтовна швидкість, Мбит/с
802.11	2.4 ГГц	1997	1
802.11b	2.4 ГГц	1999	5 (11)
802.11a	5 ГГц	2001	54
802.11g	2.4 ГГц	2003	54
802.11n	2.4 / 5 ГГц	2009	600
802.11ac	5 ГГц	2014	7000
802.11ad	60 ГГц	2009	7000
802.11ax	2.4 / 5 ГГц	2019	11 000
802.11ay	60 ГГц	В розробці	20 000

При цьому слід зазначити, що не всі перераховані стандарти Wi-Fi служать для організації бездротових локальних мереж як звичні нам роутери, що працюють в діапазонах 2.4 і 5 ГГц (стандарти 802.11 a/b/g/n/ac). Такі стандарти як 802.11 ad і 802.11 ay спочатку планувалося випустити для передачі даних на невеликі відстані - від 1 до 10 метрів – і, в перспективі, використовувати їх для організації високошвидкісних інтерфейсів передачі даних, наприклад для підключення моніторів до ПК і передачі зображення у форматі 8K. Однак, в результаті розвитку 5G-мереж і переходом в діапазон до 100 ГГц, пристрої з підтримкою 802.11 ad стали застосовуватися для організації радіодоступу поза приміщеннями (але для таких частот повинні бути забезпечені умови прямої видимості).

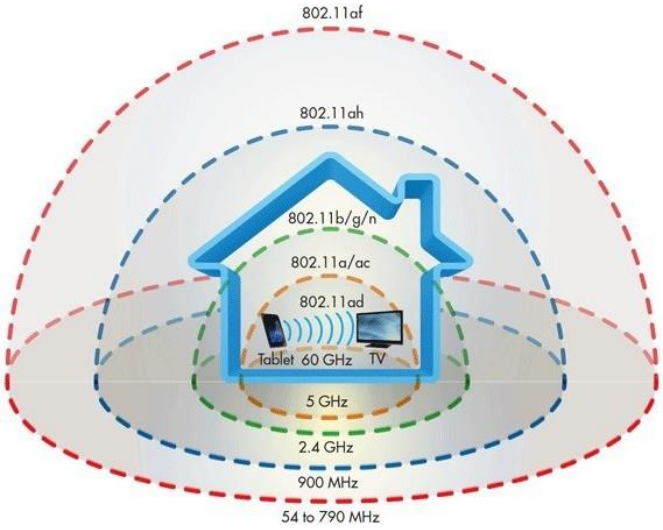


Рисунок 1.1. 1 – Вживання різноманітних стандартів Wi-Fi

1.2 Стандарти бездротового зв'язку IEEE 802

IEEE802. 11A-це перший бездротовий стандарт, що використовує OFDM на основі пакетів, заснований на пропозиції Річарда ван Ні [1] з світиться технології в Ньювегейні. OFDM був прийнятий в якості проекту стандарту 802.11 а в липні 1998 року після злиття з пропозицією NTT. Він був ратифікований в 1999 році. Стандарт 802.11 а використовує той же основний протокол, що і вихідний стандарт, працює в діапазоні 5 ГГц і використовує мультиплексування з ортогональним частотним поділом 52 піднесучих (OFDM) з максимальною швидкістю передачі необроблених даних 54 Мбіт/с, що забезпечує реалістичну чисту досяжну пропускну здатність в середині 20 Мбіт/с. Швидкість передачі даних знижується до 48, 36, 24, 18, 12, 9 потім 6 Мбіт / с, якщо потрібно. 802.11 а спочатку мав 12/13 неперекривающихся каналів, 12, які можуть використовуватися всередині приміщень, і 4/5 з 12, які можуть використовуватися в зовнішніх конфігураціях точка - точка. Останнім часом багато країн світу дозволяють роботу в діапазоні від 5,47 до 5,725 ГГц в якості вторинного користувача, використовуючи метод спільного використання, отриманий в 802.11 h. це додасть ще 12/13 каналів до загальної смузі частот 5 ГГц, що забезпечить значну загальну пропускну здатність бездротової мережі, що дозволить використовувати більше 24 каналів в деяких

країнах. 802.11 a Не сумісний з 802.11 b, оскільки вони працюють на окремих діапазонах, за винятком випадків використання обладнання, що має дводіапазонну можливість. Більшість точок доступу корпоративного класу мають дводіапазонну можливість.

Використання діапазону 5 ГГц дає 802.11 a значну перевагу, так як діапазон 2,4 ГГц сильно використовується до такої міри, що він переповнений. Деградація, викликана такими конфліктами, може призвести до частого відключення з'єднань і погіршення якості обслуговування. Однак ця висока несуча частота також приносить невеликий недолік: ефективний загальний діапазон 802.11 a трохи менше, ніж у 802.11 b / g; Сигнали стандарту 802.11 a не можуть проникати так далеко, як сигнали стандарту 802.11 b, тому що вони легше поглинаються стінами та іншими твердими об'єктами на їх шляху, а також тому, що втрата сигналу на шляху пропорційна квадрату частоти сигналу. З іншого боку, OFDM має фундаментальні переваги поширення в умовах високої багатопроменевого середовища, наприклад в приміщенні офісу, і більш високі частоти дозволяють створювати менші антени з більш високим коефіцієнтом посилення ВЧ-системи, які нейтралізують недолік більш високої смуги дії. Збільшена кількість використовуваних каналів (в 4-8 разів більше в країнах FCC) і майже повна відсутність інших заважають систем (мікрохвильові печі, бездротові телефони, радіоняні) дають 802.11 a значні сукупні переваги в пропускній здатності і надійності в порівнянні з 802.11 b/g.802.11 b має максимальну швидкість передачі необроблених даних 11 Мбіт/с і використовує той же метод доступу до носіїв CSMA/CA, визначений у вихідному стандарті. Через накладні витрати протоколу CSMA/CA на практиці максимальна пропускна здатність 802.11 b, яку може досягти додаток, становить близько 5,9 Мбіт/с при використанні TCP і 7,1 Мбіт / с при використанні UDP.

Продукти 802.11 b з'явилися на ринку в середині 1999 року, оскільки 802.11 b є прямим розширенням методу модуляції DSSS (Direct-sequence spread spectrum), визначеного в оригінальному стандарті. Apple iBook був

першим основним комп'ютером, який продавався з додатковою мережею 802.11 b. Технічно стандарт 802.11 b використовує додаткову кодову маніпуляцію (CCK) як метод модуляції, який використовує певний набір додаткових кодів довжиною 8, який спочатку був розроблений для OFDM , але також був придатний для використання в 802.11 b через його низькі властивості автокореляції з різким збільшенням пропускної здатності стандарту 802.11 b (у порівнянні з початковим стандартом) поряд з одночасним істотним зниженням цін призвело до швидкого прийняття стандарту 802.11 b в якості остаточної технології бездротової локальної мережі, а також до формування Альянсу Wi-Fi.

Пристрої стандарту 802.11 b страждають від перешкод з боку інших продуктів, що працюють в діапазоні 2,4 ГГц. Пристрої, що працюють в діапазоні 2,4 ГГц, включають в себе: мікрохвильові печі, пристрої Bluetooth, радіоняні і бездротові телефони. Проблеми з перешкодами і проблеми з щільністю користувачів в діапазоні 2,4 ГГц стали серйозною проблемою і розчаруванням для користувачів.

802.11 g є третім стандартом модуляції для бездротових локальних мереж. Він працює в діапазоні 2,4 ГГц (наприклад, 802.11 b), але працює з максимальною швидкістю передачі необроблених даних 54 Мбіт/с. Використовуючи схему передачі CSMA/CA, 31,4 Мбіт/с - це максимальна пропускна здатність мережі, можлива для пакетів розміром 1500 байт і швидкість бездротового з'єднання 54 Мбіт/с (ідентично ядру 802.11 a, за винятком деяких додаткових застарілих накладних витрат для зворотної сумісності). На практиці точки доступу можуть не мати ідеальної реалізації і тому не можуть досягти пропускної здатності навіть 31,4 Мбіт/с з пакетами по 1500 байт. 1500 байт-це звичайна межа для пакетів в Інтернеті і, отже, відповідний розмір для порівняння. Менші пакети дають ще більш низьку теоретичну пропускну здатність, аж до 3 Мбіт/с при швидкості 54 Мбіт/с і 64 байтових пакетах крім того, доступна пропускна здатність розподіляється між усіма передавальними станціями, включаючи точку доступу, тому як

низхідний, так і висхідний трафік обмежений загальним загальним обсягом 31,4 Мбіт/с з використанням 1500 байтових пакетів і швидкістю 54 Мбіт/с.

Устаткування 802.11 g повністю сумісне з обладнанням 802.11 B. деталі того, як змусити b і g добре працювати разом, займали більшу частину тривалого технічного процесу. Однак в мережі 802.11 g наявність застарілого учасника 802.11 b значно знизить швидкість всієї мережі 802.11 g. деякі маршрутизатори 802.11 g використовують режим зворотної сумісності для клієнтів 802.11 b, званий 54g LRS (підтримка обмеженої швидкості).

Схема модуляції, що використовується у 802.11 g, являє собою мультиплексування з ортогональним частотним поділом (OFDM), скопійоване з 802.11 a зі швидкістю передачі даних 6, 9, 12, 18, 24, 36, 48, і 54 Мбіт/с, і повертається до CCK (як стандарт 802.11 b) для 5,5 і 11 Мбіт/с і DBPSK/DQPSK+DSSS для 1 і 2 Мбіт/с. Незважаючи на те, що 802.11 g працює в тій же смузі частот, що і 802.11 b, він може досягати більш високих швидкостей передачі даних з-за своєї спадщини 802.11 a.

IEEE 802.11 n є поправкою до IEEE 802.11-2007 з поправками, внесеними IEEE 802.11 k-2008, IEEE 802.11 r-2008, IEEE 802.11 y-2008 і IEEE 802.11 w-2009, і грунтується на попередніх стандартах 802.11, додаючи канали з декількома входами і декількома виходами (MIMO) і 40 МГц на phy (фізичний рівень) і агрегацію кадрів на рівні Mac.

MIMO-це технологія, яка використовує кілька антен для узгодженого дозволу більшої кількості інформації, ніж це можливо за допомогою однієї антени. Одним із способів забезпечення цього є мультиплексування з просторовим поділом (SDM), яке просторово мультиплексує кілька незалежних потоків даних, переданих одночасно в межах одного спектрального каналу смуги пропускання. Mimo SDM може значно збільшити пропускну здатність у міру збільшення кількості дозволених потоків просторових даних. Для кожного просторового потоку потрібна дискретна антена як на передавачі, так і на приймачі. Крім того, технологія MIMO вимагає окремої радіочастотної ланцюга і аналого-цифрового перетворювача

для кожної антени MIMO, що робить її більш дорогою в реалізації, ніж системи без MIMO.

Канали, що працюють з шириною 40 МГц, є ще однією функцією, включеною в 802.11 n; це подвоює ширину каналу з 20 МГц в попередніх стандартах 802.11 PHYs для передачі даних і забезпечує вдвічі більшу швидкість передачі даних PHY, доступну по одному каналу 20 МГц. Він може бути включений в режимі 5 ГГц або в режимі 2,4 ГГц, якщо відомо, що він не буде заважати будь-якій іншій системі 802.11 або не 802.11 (наприклад, Bluetooth), що використовує ті ж частоти. Архітектура MIMO разом з каналами з більш широкою смугою пропускання забезпечує підвищену фізичну швидкість передачі даних по 802.11 a (5 ГГц) і 802.11 g (2,4 ГГц).

Передавач і приймач використовують методи попереднього і посткодування, відповідно, для досягнення пропускної здатності каналу MIMO. Попереднє кодування включає в себе просторове формування променя і просторове кодування, де просторове формування променя покращує якість прийнятого сигналу на етапі декодування. Просторове кодування може збільшити пропускну здатність даних за допомогою просторового мультиплексування і збільшити дальність дії за рахунок використання просторового розмаїття за допомогою таких методів, як кодування Аламуті.

Кількість одночасних потоків даних обмежена мінімальною кількістю використовуваних антен по обидві сторони лінії зв'язку. Однак окремі радіостанції часто додатково обмежують кількість просторових потоків, які можуть нести унікальні дані. Нотація A x b: c допомагає визначити, на що здатне дане радіо. Перше число (a) - це максимальна кількість передавальних антен або радіочастотних ланцюгів TX, які можуть використовуватися радіостанцією. Друге число (b) - це максимальна кількість приймальних антен або радіочастотних ланцюгів RX, які можуть використовуватися радіостанцією. Третє число (c) - це максимальна кількість просторових потоків даних, які може використовувати радіо. Наприклад, радіо, яке може

передавати на двох антенах і приймати на трьох, але може відправляти або приймати тільки два потоки даних, буде 2 x 3 : 2.

Проект 802.11 n допускає до 4 x 4 : 4. Поширеними конфігураціями пристроїв 11n є 2x2: 2, 2x3: 2 і 3x2: 2. Всі три конфігурації мають однакову максимальну пропускну здатність і характеристики і відрізняються тільки ступенем рознесення, що забезпечується антенними системами. Крім того, стає поширеною четверта конфігурація, 3x3:3, яка має більш високу пропускну здатність через додатковий потік даних.

Припускаючи, що робочі параметри мережі 802.11 g дорівнюють 54 мегабітам в секунду (на одному каналі 20 МГц з однією антеною), мережа 802.11 n може досягати 72 мегабіт в секунду (на одному каналі 20 МГц з однією антеною і інтервалом захисту 400 нс); швидкість 802.11 n може досягати 150 мегабіт в секунду, якщо поблизу немає інших випромінювань Bluetooth, мікрохвильової печі або Wi-Fi, використовуючи два канали 20 МГц в режимі 40 МГц. Якщо використовується більше антен, то 802.11 n може досягати 288 мегабіт в секунду в режимі 20 МГц з чотирма антенами або 600 мегабіт в секунду в режимі 40 МГц з чотирма антенами і інтервалом захисту 400 нс. Оскільки діапазон 2,4 ГГц серйозно перевантажений в більшості міських районів, мережі 802.11 n зазвичай досягають більшого успіху в збільшенні швидкості передачі даних, використовуючи більше антен в режимі 20 МГц, а не працюючи в режимі 40 МГц, оскільки режим 40 МГц вимагає відносно вільного радіочастотного спектру, який доступний тільки в сільських районах далеко від Міст. Таким чином, мережеві інженери, які встановлюють мережу 802.11 n, повинні прагнути вибирати маршрутизатори і бездротові клієнти з максимально можливою кількістю антен (одна, дві, три або чотири, як зазначено в стандарті 802.11 n) і намагатися переконатися, що пропускна здатність мережі буде задовільною навіть в режимі 20 МГц.

Швидкість передачі даних до 600 Мбіт/с досягається тільки при використанні максимум чотирьох просторових потоків з використанням одного каналу шириною 40 МГц. Різні схеми модуляції і швидкості кодування

визначаються стандартом і представлені значенням індексу схеми модуляції і кодування (MCS). У таблиці нижче показані взаємозв'язки між змінними, які забезпечують максимальну швидкість передачі даних. GI (захисний інтервал): час між символами.

Канал 20 МГц використовує БПФ з 64, з яких: 56 піднесуть OFDM, 52 призначені для передачі даних і 4 є пілотними тонами з поділом несучих 0,3125 МГц (20 МГц/64) (3,2 мкс). Кожен з цих піднесення може бути BPSK, QPSK, 16-QAM або 64-QAM. Загальна смуга пропускання становить 20 МГц при займаній смузі пропускання 17,8 МГц. Загальна тривалість символу становить 3,6 або 4 мікросекунди, що включає захисний інтервал 0,4 (також відомий як короткий захисний інтервал (SGI)) або 0,8 мікросекунди.

Швидкість передачі даних на рівні PHY не відповідає пропускній здатності на рівні користувача через накладні витрати протоколу 802.11, таких як процес конкуренції, міжкадрова відстань, заголовки рівня PHY (преамбула + PLCP) і кадри підтвердження. Основною функцією управління доступом до Мультимедіа (MAC), що забезпечує підвищення продуктивності, є агрегування. Визначено два типи агрегування:

Агрегація одиниць даних служби MAC (MSDU) у верхній частині MAC (звана агрегацією MSDU або A-MSDU)

Агрегація блоків даних протоколу MAC (MPDU) в нижній частині MAC (звана агрегацією MPDU або A-MPDU)

Агрегація кадрів - це процес упаковки декількох MSDU або MPDU разом, щоб зменшити накладні витрати і усереднити їх по декількох кадрах, тим самим збільшуючи швидкість передачі даних на рівні користувача. Агрегація A-MPDU вимагає використання блочного підтвердження або BlockAck, який був введений в 802.11 e і оптимізований в 802.11 n.

Коли 802.11 g був випущений для спільного використання смуги частот з існуючими пристроями 802.11 b, він забезпечив способи забезпечення співіснування між успадкованими і наступними пристроями. 802.11 n розширює управління співіснуванням для захисту своїх передач від застарілих

пристроїв, які включають 802.11 g, 802.11 b і 802.11 a. існують механізми захисту на рівні MAC і PHY, перераховані нижче:

Захист рівня PHY: захист формату змішаного режиму(також відомий як захист L-SIG TXOP): у змішаному режимі кожна передача 802.11 n завжди вбудована в передачу 802.11 a або 802.11 g. для передач з частотою 20 МГц це вбудовування забезпечує захист за допомогою стандартів 802.11 a і 802.11 g. однак пристрої 802.11 b як і раніше потребують захисту CTS.

Захист рівня PHY: передачі з використанням каналу 40 МГц в присутності клієнтів 802.11 a або 802.11 g вимагають використання захисту CTS на обох половинах каналу 40 МГц з частотою 20 МГц для запобігання перешкод застарілим пристроям.

Захист на рівні MAC: обмін кадрами RTS / CTS або передача кадрів CTS за застарілими швидкостями можуть використовуватися для захисту подальшої передачі 11n.

1.3 Режими роботи бездротових мереж Wi-Fi

У цьому режимі пристрій підключається до провідної мережі і перетворює сигнал в бездротовий.

Рисунок 1.3.1 – Режим точка доступу

В даному режимі пристрій розширює зону покриття батьківської мережі Wi-Fi, шляхом її ретрансляції (повторення). Існує окремий тип точок доступу, який так і називають повторювачі або розширювачі бездротової мережі. Деякі моделі можуть працювати тільки в цьому режимі, а деякі і, наприклад, в режимі точки доступу.

Рисунок 1.3.2 – Режим повторювача

У режимі клієнта точка доступу працює як бездротовий мережевий адаптер, отримуючи сигнал бездротової мережі. Клієнти підключаються до порту LAN.

Рисунок 1.3.3 – Режим клієнта

Дозволяє бездротовій точці обмінюватися даними з іншою точкою доступу (маршрутизатором), використовується для з'єднання двох віддалених дротових мереж, за допомогою Wi-Fi.

Рисунок 1.3.4 – Бездротовий міст

Аналогічний попередньому режиму, але додатково дозволяє створити локальну бездротову мережу для всіх пристроїв Wi-Fi.

Multi-SSID: у цьому режимі пристрій може створити до 4 бездротових мереж, позначених різними SSID, і призначити кожному SSID різні налаштування безпеки або VLAN. Особливо корисно в ситуації, коли потрібні різні політики доступу і функції.

Рисунок 1.3.5 – Міст через з точкою доступу

Точки доступу Wi-Fi в даний час використовують дві основні частоти: 2.4 ГГц і 5 ГГц. Зазвичай більш дешеві пристрої використовують тільки 2.4 ГГц діапазон, більш дорогі 5 ГГц, або обидва відразу.

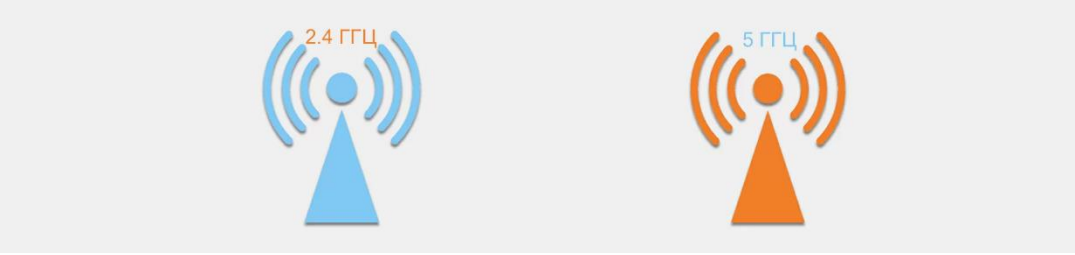


Рисунок 1.3.6 – Частотний діапазон

Перевага 5 ГГц мереж полягає в більшій швидкості з'єднання і менш "зашумленном" діапазоні, а перше дуже сильно залежить від другого. 5 ГГц точок доступу менше, вони дорожче, сигнал загасає швидше, тому сусідські точки доступу менше впливатимуть на вашу мережу. Також тут немає інших

джерел перешкод, характерних для 2.4 ГГц діапазону: СВЧ-печей, Bluetooth-пристроїв (мишки, клавіатури, гарнітури, колонки), радіонянь.

За час свого існування С 1996 року Wi-Fi (точніше IEEE 802.11), як і будь-яка технологія, пройшла кілька стадій свого розвитку. Відповідно з'являлися і різні її версії. Тестування на сумісність і сертифікацією бездротових пристроїв, займається окрема організація WECA (Wireless Ethernet Compatibility Alliance) більш відома як Wi-Fi Alliance.

Wi-Fi 802.11-перша версія стандарту. Швидкість передачі даних до 1 Мбіт/с (після удосконалення технології - 2 Мбіт/с), діапазон — 2.4 ГГц;

Wi-Fi 802.11a - швидкість до 54 Мбіт/с, діапазон-5 ГГц;

Wi-Fi 802.11b - пропускна здатність від 5.5 до 11 Мбіт/с, діапазон - 2.4 ГГц;

Wi-Fi 802.11g - швидкість до 50 Мбіт/с, діапазон - 2.4 ГГц, сумісність з 802.11b;

Wi-Fi 802.11n - підтримуються і 2.4 і 5 ГГц діапазон, сумісний з 802.11 a/b/g. Максимальна швидкість до 600 Мбіт/с, при використанні технології MIMO;

Wi-Fi 802.11ac - діапазон-5 ГГц, пропускна здатність від 433 Мбіт/с до 6.77Гбіт / с. технологія MIMO еволюціонувала до MU-MIMO;

Wi-Fi 802.11ad-експлуатує частоту в 60 ГГц, пропускна здатність до 7 Гбіт / с;

Wi-Fi 802.11ax-повинен прийти на зміну 802.11ac, мережі — 2.4 і 5 ГГц, а також використовувати додаткові канали в діапазоні від 1 до 7 ГГц. Обіцяно багато поліпшень: від збільшення пропускної здатності, до зменшення затримок і більш кращої роботи в умовах щільної забудови.

Wi-Fi Alliance планує перехід на інший, більш зручний для користувачів, формат назви поколінь: замість 802.11 ax буде використовуватися Wi-Fi 6, 802.11 ac — Wi-Fi 5, 802.11 n — Wi-Fi 4.

У міру впровадження нових версій стандарту збільшувалася максимальна пропускна здатність Wi-Fi, причому як інтенсивними

(збільшення швидкості на 1 антену), так і екстенсивними (збільшенням кількості антен) методами. Заявлені цифри наведені в таблиці:

Таблиця 1.3.1 – Максимальна пропускна здатність Wi-Fi

802.11a	до 54 Мбит/с
802.11b	до 11 Мбит/с
802.11g	до 54 Мбит/с
802.11n	до 600 Мбит/с
802.11ac	до 6.77 Гбит/с

Але навіть якщо пристрій, на якому, наприклад, гордо буде вказана швидкість до 300 Мбіт/с, то ви отримаєте максимум 50-60% від заявленої величини. При збільшенні відстані між приймачем і передавачем, появі перешкод на шляху проходження сигналу, ця величина стане ще менше.

Розрізняють внутрішні-розташовані в корпусі пристрою і зовнішні антени. Внутрішні не збільшують габарити пристрою, але в більшості своїй менш потужні, ніж зовнішні і орієнтовані в просторі тільки в одному положенні. Зовнішні мають шарнір з декількома ступенями свободи, що дозволяє повернути або відхилити антену в потрібне положення.

Зовнішні, в свою чергу, можуть бути знімними і не знімними. Перевагою знімних моделей є можливість їх заміни на аналогічні, з великим коефіцієнтом посилення або інший діаграмою спрямованості, в разі пошкодження або бажання збільшити радіус дії мережі. Також зовнішні антени розрізняються конструктивно: якщо раніше це був спеціальний провідник, то зараз нерідко використовуються друковані плати.

При описі стандартів Wi-Fi швидкість передачі даних варіюється в залежності від кількості антен. Так в стандарті n максимальне число антен одно 4, A B ac — 8. Але пристрій приймає сигнал від точки доступу також повинен оснащуватися такою ж кількістю антен, інакше швидкість буде обмежена стороною з меншою їх кількістю. Але в будь-якому випадку, більша кількість антен додає дальності Wi-Fi.

Збільшення пропускної здатності Wi-Fi мережі при використанні декількох антен, описане трохи вище, з'явилося завдяки впровадженню технології MIMO.

MIMO-це технологія одночасної передачі декількох інформаційних потоків по одному бездротовому каналу. У стандарті 802.11 n використовувався SU-mimo (Single-user MIMO) і він відмінно працював, коли клієнт в мережі тільки один. Якщо ж клієнтів ставало хоча б 2, то точка доступу обслуговувала їх по черзі, що аж ніяк не додавало швидкості.

Тому в стандарті 802.11 ac Wave 2 з'явився вдосконалений варіант MU-MIMO (Multi-user MIMO). Тепер точка доступу може одночасно передавати дані на кілька (по числу використовуваних антен) пристроїв, що дозволяє більш повно використовувати пропускну здатність мережі, поліпшити якість голосових VOIP і відеодзвінків.

Сучасні точки доступу пропонують кілька типів стандарту шифрування.

WEP-з'явився найпершим, на сьогоднішній день використання його вкрай не рекомендується, зважаючи на його ненадійність. WPA - і WPA2 зокрема, є більш досконалими алгоритмами на сьогоднішній день. Всі сучасні точки доступу використовують даний стандарт, зламати його набагато важче, але все ж, чим більше символів (букв, цифр, спецсимволів) буде містити ваш пароль тим краще. Стандарт, рекомендує використовувати послідовність з не менше ніж 20 символів, інакше пароль вважається не надійним.

У професійних моделях передбачені й інші способи захисту доступу: наприклад, доступ до мережі з використанням персональних сертифікатів.

Для точок доступу характерний тільки один порт LAN, який призначається для підключення до існуючої провідної мережі, або до клієнтського пристрою, в залежності від режиму роботи. У бюджетних моделях, швидкість дротового підключення обмежена 100 Мбіт/с. у більш дорогих моделях використовують порти з пропускною здатністю 1 Гбіт/с, що необхідно як для доступу в Інтернет на тарифах понад 100 Мбіт/с, але і для

організації швидкої локальної мережі як провідний, так і бездротової (при використанні стандарту 802.11 ac).

Технологія, що дозволяє передавати по Ethernet кабелю не тільки інформацію, але і харчування для роботи пристрою. Дуже корисна річ, особливо для вуличних варіантів або моделей для великих приміщень, зважаючи на специфіку їх розташування.

Один з найчастіших питань у покупців, це яку площу покриє сигнал від точки доступу, і чому цих даних немає в характеристиках. Але цей показник залежить від стількох параметрів, що порахувати його дуже проблематично. І якісь приблизні цифри можна сказати, лише маючи деякий практичний досвід. Однак деякі речі можна констатувати однозначно.

Будь-які перешкоди знижують потужність сигналу, тим самим зменшуючи радіус покриття мережі;

Відповідно до закону фізики сигнал мережі 2.4 ГГц діапазону менше гаситься, проходячи через перешкоду, ніж аналогічний за потужністю сигнал від 5 ГГц випромінювача;

Сигнали від інших точок доступу також будуть "заважати" сигналу вашого пристрою.

2 РЕАЛІЗАЦІЯ МЕРЕЖІ БЕСПРВОДНОГО ДОСТУПУ

2.1 Місце реалізації проекту

За основу для проектування телекомунікаційної мережі Було взято підприємство П - образної форми (рис 2.1.1).

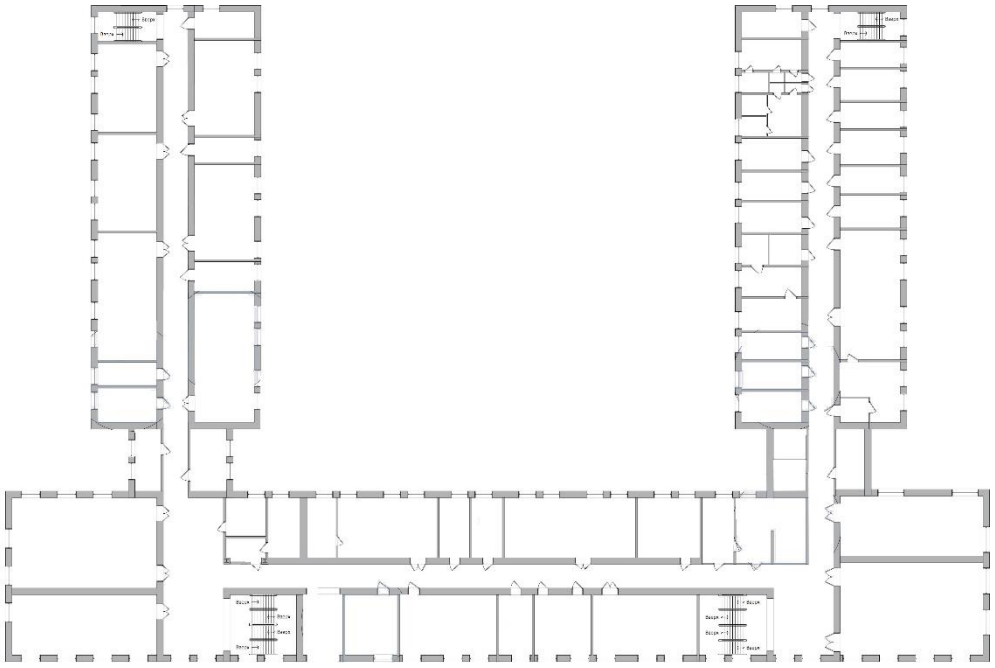


Рисунок 2.1.1 – Схема

Необхідність і актуальність організації мережі бездротового доступу, на базі технології Wi-Fi, на підприємстві, обумовлена зростаючою потребою до підвищення рівня інформатизації. Рівень інформатизації можна підвищити за допомогою сучасних послуг зв'язку: високошвидкісний доступ в Інтернет, комп'ютерна мережа.

Для задоволення потреби буде використовуватися обладнання на базі стандарту 802.11n (Wi-Fi).

Завдання проекту:

- Розгортання мережі бездротового доступу Wi-Fi

- Задоволення існуючого і прогнозованого попиту на послуги телекомунікацій.
- Підвищення рівня інформатизації.
- Область застосування технологій бездротового доступу Wi-Fi:
- Економічна недоцільність підключення по провідній лінії;
- Швидкий захоплення потенційних абонентів.
- Забезпечення високої швидкості передачі даних.

2.2 Вибір обладнання

Проект базується на обладнанні с підтримкою стандарту 802.11n, який отримав сертифікат Wi-Fi. Wi-Fi покриває всю територію підприємства і об'єднує всіх користувачів в єдину мережу з доступом в інтернет. Мережа здійснюється встановленими по всій території підприємства бездротовими уніфікованими точками доступу.

2.2.1 Роутер Xiaomi Mi WiFi Router 4A

Роутер працює в двох частотних діапазонах: 2,4 ГГц і 5 ГГц. Сигнали будуть накладатися один на одного і не будуть створювати перешкоди. Швидкість передачі даних може досягати 1167 Мбіт / с. Частотний діапазон 2,4 ГГц має велику площу покриття і кращу прохідність крізь стіни. Технологія 802.11ac працює тільки на частоті 5 ГГц. Пристрої на частоті 5 ГГц відчувають менше перешкод, а швидкість в цьому діапазоні помітно вище.

Роутер Xiaomi Mi Wi-Fi Router 4A підтримує одне ім'я мережі для діапазонів 2,4 ГГц і 5 ГГц. Тепер більше не виникне плутанини з підключенням до мережі. Частота 2,4 ГГц має кращу прохідність крізь стіни, а частота 5 ГГц має велику швидкість передачі даних. Вибирайте частоту, яка підходить саме Вам.

Роутер Xiaomi Mi оснащений 4 всеспрямованими антенами з високим коефіцієнтом посилення. Висока швидкість передачі даних досягається завдяки багаторазовим тестуванням, складну внутрішню структуру роутера і

його організації. Роутер забезпечить стабільний сигнал навіть в найскладніших умовах.

Поєднання металевої підкладки, обробленої спеціальним чином, і наноматеріалів, що володіють хорошою провідністю, сприяє відмінному розподілу температури і ефективному охолодженню, що забезпечує стабільну роботу роутера.

Діапазони частот 2,4 Ггц, і 5 Ггц працюють спільно з вбудованими чіпами PA і LNA. PA (підсилювач потужності) збільшує потужність передачі сигналу, LNA (малошумний підсилювач) може поліпшити чутливість прийому сигналу. Чим більше відстань передачі сигналу від Wi-Fi-роутера до точки прийому, тим прохідність крізь стіни буде краще, а зона охоплення ширше.

Всі пристрої "розумного будинку" вимагають стабільного підключення. Роутер Xiaomi Mi Wi-Fi Router 4A наділений великим обсягом внутрішньої пам'яті (64 Мб), що забезпечує стабільну передачу даних і безпечне з'єднання між пристроєм і роутером.

При зміні пароля в додатку Xiaomi роутер Xiaomi Mi Wi-Fi Router 4A автоматично синхронізується з пристроєм, підключеним до системи "розумний будинок". Що означає, що після зміни пароля, Вам не потрібно буде міняти його для кожного пристрою окремо.

IPv6 має збільшене адресний простір, завдяки чому користуватися Інтернетом стало набагато простіше. Роутер Xiaomi Mi Wi-Fi Router 4A підтримує IPv6, що полегшує доступ до освітніх ресурсів. Підготуйтеся до майбутнього розгортання IPv6-мережі.

Діапазон частот 5 ГГц підтримує алгоритм корекції помилок LDPC (код з малою щільністю перевірок на парність), який покращує захист від перешкод в каналі передачі даних, а також значно збільшує площу покриття сигналом Wi-Fi і підвищує ефективність передачі даних.

Захистіть свою родину від негативного контенту, включивши функцію обмеження за часом і задавши діапазон дозволених URL-адрес. Ви можете

встановити обмеження швидкості на роутері для кожного пристрою, щоб уникнути перевантаження мережі.

Якщо до Вашого роутера підключилося стороннє пристрій, додаток Xiaomi відправить Вам повідомлення. У разі підключення до роутера пристрої з високим рівнем ризику маршрутизатор самостійно обмежить доступ до мережі або відправить Вам нагадування.

Додаток Xiaomi включає в себе безліч корисних функцій, таких як вимірювання швидкості, оптимізація з'єднання, захист від незаконного підключення. Ви також зможете віддалено змінювати налаштування роутера, управляти підключеними пристроями та багато іншого. Відкрийте програму і почніть користуватися.

Завдяки співпраці з такими міжнародними компаніями з виробництва тестових приладів, як Spirent, Ixia і численним випробуванням, що імітує роботу роутера в домашніх і екстремальних умовах, гарантується стабільна робота пристрою при будь-яких обставинах.

Корпус має просту геометричну форму. Він виконаний з матового білого пластику. Роутер має стильний і привабливий дизайн, який чудово впишеться в будь-який інтер'єр будинку. Корпус і упаковка роутера Xiaomi Mi Wi-Fi Router 4A виготовлені з нешкідливих матеріалів, які легко утилізуються і переробляються. [16]

Рисунок 2.1.2 – Router 4A

Таблиця 2.2.1 – характеристики обладнання

Бренд	Readme
Модель	AX 5
Процесор	Одноядерний MT7628DA
Оперативна пам'ять:	16 МБ
Пам'ять	64 МБ
Wi-Fi 2.4G:	2 x 2 (протокол IEEE 802.11 N, швидкість 300 Мбіт / с)
Wi-Fi 5G:	2 x 2 (протокол IEEE 802.11 AC, швидкість 867 Мбіт / с
Антена	2 x 2.4 ГБ / 5 дбі + 2 x 5 ГБ / 6 дбі
Інтерфейс	2 x 10/100 LAN (Auto MDI / MDIX)
Діапазон	1 x 10/100 WAN порт (Auto MDI / MDIX)
Безпека	
Бездротовий канал:	2.4 ГГц і 5 ГГц
Спосіб модуляції:	11b: DSSS: DBPSK (1 Мбіт / с), DQPSK (2 Мбіт / с), CCK (5,5 / 11 Мбіт / с) 11A / g: OFDM: BPSK (6/9 Мбіт / с), QPSK (12/18 Мбіт / с), 16 QAM (24/36 Мбіт / с), 64QAM (48) / 54 Мбіт / с) 11n: MIMO-OFDM: BPSK, QPSK, 16QAM, 64QAM. Набір швидкості: MCS0 ~ MCS15 11ac: MIMO-OFDM: BPSK, QPSK, 16QAM, 64QAM, 256QAM. Набір швидкості: MCS0 ~ MCS9 (підтримує 2 потоки)
Розмір	175 x 188 мм

2.2.2 Беспроводной роутер Xiaomi Redmi AX5

Redmi AX5 використовує 5-ядерний процесор Qualcomm, виготовлений за технологією 14 нм, і модуль NPU, щоб прискорити апаратну обробку.

Маршрутизатор AX5 використовує 4-ядерний чіп IP53 A53 з частотою 1.2 ГГц і 1-ядерний модуль NPU 1.5 ГГц для підвищення обчислювальної потужності на 130%, оптимізації мережевих даних і перегляду відео в дозволі 4k.

Він має ПЗУ 128 МБ і ОЗУ 256 МБ для можливості одночасного підключення до 128 пристроїв, підтримки підключення до девайсів «розумного будинку», підвищення конфіденційності.

Це перший маршрутизатор від бренду Redmi використовує технологію Wi-Fi 6. Він здатний забезпечити швидкість передачі на 52% вище, ніж маршрутизатор AC1200 Wi-Fi 5, що дозволяє завантажувати HD-відео всього за 8 секунд з досягнутою швидкістю 1775 Мбіт/с.

Маршрутизатор Redmi AX5 також підтримує технологію OFDMA, яка дозволяє передавати дані на 8 пристроїв тільки з однією лінією передачі, знижуючи затримку до 66%.

Роутер Redmi AX5 підтримує діапазони 2.4 / 5 ГГц одночасно з незалежним підсилювачем сигналу Qorvo, який підсилює сигнал на 4 дБ.

Redmi AX5 обладнаний 4 всеспрямованими антенами 5 дбі і алгоритмом корекції помилок LDPC, який значно розширює можливості захисту від перешкод і покриття сигналу під час передачі даних.

У смузі 5 ГГц роутер підтримує мережеве з'єднання відповідно до моделі комірчастої мережі і змішаної мережею зі швидкістю до 1201 Мбіт/с.

Wi-Fi Router AX5 оснащений технологією MU-MIMO для поліпшення зв'язку, коли кілька пристроїв працюють одночасно. Також, пристрій обладнаний технологією алгоритмів, яка оптимізує можливість передачі BSS Coloring, що допомагає зменшити перешкоди між різними системами Wi-Fi, забезпечуючи кращий користувальницький досвід.

Таблиця 2.2.2 – характеристики обладнання

Бренд	Redmi
Модель	AX5
Конфігурація	CPU IPQ6000 з 4 ядрами A53 1.2 ГГц Одноядерний модуль CPU 1.5 ГГц 128 МБ ПЗУ 256 МБ ОЗУ
Wi-Fi 2.4G:	2x2 (протокол 802.11 ac, максимальна швидкість 574 Мбіт / с)
Wi-Fi 5G:	2x2 (протокол 802.11 ac, максимальна швидкість 1201 Мбіт / с)
Антена	4 зовнішні антени
Інтерфейс	Один адаптивний порт WAN 10 / 100 /1000M (Auto MDI / MDIX) Три адаптивні порти LAN 10 / 100 / 1000M (Auto MDI / MDIX)
Діапазон	2.4 ГГц і 5 ГГц
Безпека	WPA-PSK / WPA2-PSK / WPA3-SAE
Бездротовий канал:	2.4 ГГц канал: 1,2,3,4,5,6,7,8,9,10,11,12,13 5 ГГц канал: 36,40,44,48,149,153,157,161,165
Спосіб модуляції:	11b: DSSS: DBPSK (1 Мбіт / с), DQPSK (2 Мбіт / с), CCK (5,5 / 11 Мбіт / с) 11A / g: OFDM: BPSK (6/9 Мбіт / с), QPSK (12/18 Мбіт / с) 16KAM (24/36 Мбіт / с), 64KAM (48/54 Мбіт / с) 16KAM (24/36 Мбіт / с), 64KAM (48/54 Мбіт / с) 11n: MIMO-AFDM: B-PSG, QPSK, 16QAM, 64QAM 11ac: MIMO-AFDM: BPSK, QPSK, 16QAM, 64QAM, 256QAM. MCS0 ~ MCS9 (підтримує 2 потоки) 11ax: MIMO-AFDM: BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM. MCS0 ~ MCS11 (підтримує 2 потоки)
Розмір	247 x 141 x 180 мм

Технологія Beamfornming також інтегрована для автоматичного виявлення пристроїв, які використовують Wi-Fi для поліпшення покриття.

Крім того, маршрутизатор Redmi оснащений новітніми протоколами безпеки WPA3 і Ipv6, які допомагають захистити інформацію і дані Користувача.[17]

Рисунок 2.1.2 – Redmi AX5

2.2.3 Маршрутизатор Xiaomi AIoT Router AX3600

Маршрутизатор Xiaomi AIoT Router AX3600 використовує стандарт Wi-Fi 6, з максимальною пропускною здатністю 9.6 Гбіт / с.з точки зору швидкості, Wi-Fi 6 в 2.7 рази більше, ніж у Wi-Fi 5 і в 16 разів більше, ніж у Wi-Fi 4.

Що стосується апаратного забезпечення, AX3600 обладнаний чіпом Qualcomm IPQ8071A і 512 МБ пам'яті. Чіп використовує 4-ядерну архітектуру A53, тактову частоту 1 ГГц, а також інтегрує двоядерний чіп процесора мережевого прискорення NPU, тому також говориться, що AX3600 оснащений 6-ядерним чіпом.

Маршрутизатор AX3600 підтримує протоколи шифрування OFDMA, MU-MIMO, BSS Coloring, Beamforming і IPv6 і WPA3 і відрізняється

хорошими здібностями зменшення перешкод сигналу, підвищення ефективності зв'язку та безпеки, розширення адресного простору мережі.

Крім того, AX3600 також має вбудований плагін прискорення NetEase UU, який підтримує глобальні функції мережевого прискорення ігрових консолей, таких як PS4, Switch і Xbox One, скорочуючи затримку онлайн-битв.

Стандарт Wi-Fi 6 був випущений в 2019 році і підтримує діапазон від 1 ГГц до 6 ГГц, включаючи використовувані в даний час смуги частот 2.4 ГГц і 5 ГГц, зі зворотною сумісністю a/b/g/n/ac. Завдяки впровадженню MU-MIMO, модуляції 1024qam, 8 x 8 MIMO та інших технологій теоретична максимальна швидкість Wi-Fi 6 досягає показника в 9.6 Гбіт/с. [19]

Рисунок 2.1.2 – Redmi AX3600

Таблиця 2.2.3 – характеристики обладнання

Бренд	Redmi
Модель	AX3600
Процесор	IPQ8071A 4-ядерний процесор A53 1 ГГц 2-ядерний мережевий прискорювач 1.7 ГГц NPU
Оперативна пам'ять:	256 МБ
Wi-Fi 2.4G:	2 x 2 (підтримує протокол IEEE 802.11 ac на найвищому рівні, теоретична максимальна швидкість може досягати 574 Мбіт / с)
Wi-Fi 5G:	4 x 4 (підтримує протокол IEEE 802.11 ac до теоретичної максимальної швидкості 2402 Мбіт / с)
Стандарт протоколу:	IEEE 802.11a / b / g / n / ac / ax, IEEE 802.3 / 3u / 3ab
Антена	6 вбудованих антен з високим коефіцієнтом посилення + 1 зовнішня антена Yota
Інтерфейс	Один 10 / 100 / 1000M адаптивний порт WAN (Auto MDI / MDIX) Три адаптивні порти LAN 10 / 100 / 1000M (Auto MDI / MDIX)
Діапазон	2.4 ГГц і 5 ГГц
Безпека	WPA-PSK / WPA2-PSK / WPA3-SAE
Бездротовий канал:	2.4 ГГц канал: 1,2,3,4,5,6,7,8,9,10,11,12,13 5 ГГц канал: 36,40,44,48,149,153,157,161,165
Спосіб модуляції:	11b: DSSS: DBPSK (1 Мбіт / с), DQPSK (2 Мбіт / с), CCK (5.5 / 11 Мбіт / с) 11A / g: OFDM: BPSK (6/9 Мбіт / с), QPSK (12/18 Мбіт / с), 16 QAM (24/36 Мбіт / с), 64QAM(48/54 Мбіт / с) 11n: MIMO-OFDM: BPSK, QPSK, 16QAM, 64QAM. Встановлена швидкість: MCS0 ~ MCS1511ac 11ac: MIMO-OFDM: BPSK, QPSK, 16QAM, 64QAM, 256QAM. Встановлена швидкість: MCS0 ~ MCS9 (підтримує 4 потоки) 11ax: MIMO-OFDM: BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024qam. Швидкість набору: MCS 0 ~ MCS 11 (Підтримка 4 потоків)
Розмір	410 x 177 x 134 мм

2.3. Розрахунок дальності роботи бездротового каналу зв'язку 802.11

Розрахунок дальності бездротового каналу Wi-Fi виводиться з формули (2.1) розрахунку втрат у вільному просторі.

$$FSL = 33+20(\lg F +\lg D), \quad (2.1)$$

де FSL (Free Space Loss) - втрати у вільному просторі (дБ);

F - центральна частота каналу, на якому працює система зв'язку (МГц);

D - відстань між двома Wi-Fi точками (км).

Отже, шукане відстань D можна визначити за формулою (2.2).

$$D = 10^{\frac{FSL-33}{20}-\log F} \quad (2.2)$$

Втрати у вільному просторі також можна визначити за формулою (2.3), виходячи з сумарного посилення системи передачі УдБ.

$$FSL = Y_{\text{дБ}} - SOM, \quad (2.3)$$

де SOM (System Operating Margin) - запас в енергетиці радіозв'язку (дБ), який враховує можливі фактори, що негативно впливають на дальність зв'язку.

Параметр SOM зазвичай береться рівним 10 дБ. Вважається, що такий запас щодо посилення достатній для інженерного розрахунку.

Сумарне посилення системи передачі розраховується за формулою (2.4).

$$Y\text{дБ} = Pt,\text{дБм} + Gt,\text{дБи} - P\text{min}, \quad (2.4)$$

де Pt, дБм - потужність передавача (паспортні дані пристрої);

Gt, дБи - коефіцієнт посилення передавальної антени (паспортні дані пристрої);

Pmin, дБм - чутливість приймача на даній швидкості;

У табл.2.4.1 наведені середні показники чутливості для різних швидкостей передачі даних в діапазоні 2,4 ГГц для 802.11g і 5 ГГц для 802.11n (канал 40 МГц).[22]

Таблиця 2.3.1 – Залежність чутливості від швидкості передачі даних для 802.11g і 802.11n

Швидкість Мбит/с	Чутливість дБм	Швидкість Мбит/с	Чутливість дБм
802.11g 2,4 ГГц			
54	−66	18	−83
48	−71	12	−85
36	−76	9	−86
24	−80	6	−87

Визначимо Xiaomi Mi WiFi Router 4A дальність роботи каналу зв'язку для технології 802.11n в 40 МГц каналі, що об'єднує канали 1, при швидкості передачі, що дорівнює 54 Мбіт/с.

Початкові дані.

• Потужність передавача Pt, дБм = 19 дБм

• Коефіцієнт посилення штатної антени передавача Gt, дБи = 5 дБі.

Визначимо сумарний посилення системи передачі за формулою (2.4).

$Y_{дБ}$= 19+5−(−66) = 90 дБ.

За формулою (2.3) визначимо втрати у вільному просторі.

FSL = 90−10 = 80 дБ.

Таблиця 2.3.2 – Центральні частоти каналів 802.11 в діапазоні 2,4 ГГц

Номер каналу	Частота МГц	Номер каналу	Частота МГц	Номер каналу	Частота МГц	Номер каналу	Частота МГц
1	2412	5	2432	9	2452	13	2472
2	2417	6	2437	10	2457	14	2484
3	2422	7	2442	11	2462		
4	2427	8	2447	12	2467		

Центральна смуга частот об'єднаного 40 МГц каналу 1 згідно табл.2.4.2 буде дорівнювати

F = 2412 МГц.

Розрахуємо шукане відстань, згідно з формулою (2.2).

$D = 10^{\frac{80-33}{20}-\log 2412} = 0{,}091$км ≈ 91 м.

Визначимо Xiaomi Redmi AX5 дальність роботи каналу зв'язку для технології 802.11n в 40 МГц каналі, що об'єднує канали 1, при швидкості передачі, що дорівнює 54 Мбіт/с.

Початкові дані.

• Потужність передавача Pt, дБм = 23 дБм

• Коефіцієнт посилення штатної антени передавача Gt, дБи = 5 дБі.

Визначимо сумарний посилення системи передачі за формулою (2.4).

$Y_{дБ} = 23+5-(-66) = 94$ дБ.

За формулою (2.3) визначимо втрати у вільному просторі.

$FSL = 94-10 = 84$ дБ.

Центральна смуга частот об'єднаного 40 МГц каналу 1 згідно табл.2.4.2 буде дорівнювати

F = 2412 МГц.

Розрахуємо шукане відстань, згідно з формулою (2.2).

$D = 10^{\frac{84-33}{20}-\log 2412} = 0{,}147$км ≈ 147 м.

Визначимо Xiaomi AIoT Router AX3600 дальність роботи каналу зв'язку для технології 802.11n в 40 МГц каналі, що об'єднує канали 1, при швидкості передачі, що дорівнює 54 Мбіт/с.

Початкові дані.

• Потужність передавача Pt, дБм = 30 дБм

• Коефіцієнт посилення штатної антени передавача Gt, дБи = 6 дБі.

Визначимо сумарний посилення системи передачі за формулою (2.4).

$Y_{дБ} = 30+6-(-66) = 102$ дБ.

За формулою (2.3) визначимо втрати у вільному просторі.

$FSL = 102-10 = 92$ дБ.

Центральна смуга частот об'єднаного 40 МГц каналу 1 згідно табл.2.4.2 буде дорівнювати

F = 2412 МГц.

Розрахуємо шукану відстань, згідно з формулою (2.2).

$D = 10^{\frac{92-33}{20}-\log 2412} = 0{,}369$км ≈ 369 м.

З розрахуноку дальності роботи бездротового каналу зв'язку 802.11(2,4ГГц).

Було виявлено що Xiaomi AIoT Router AX3600 має досить велику відстань покриття 369м. Роутер Xiaomi Redmi AX5 має меншу відстань покриття 144м. Найгірший результат показав роутер Xiaomi Router 4A 92м.

Оптимальна кількість роутерів після розрахунку дальності роботи бездротового каналу зв'язку 802.11 дорівнює 4 пристрої. Дані пристрої будут розташовані в такій послідосності по одному пристрою в кожне крило будівлі і два в центральній частині будівлі. З паспортних даних пристрою ми знаємо максимальну кількість користувачів в мережі і знаючи потрібне нам кількість роутерів для оптимального покриття всього поверху будівлі ми можемо підрахувати скільки максимально може підключиться людей до мережі.

Таблица 2.3.3 – Допустима кількість користувачів

Назва пристрою	1 роутер	4 роутера
Xiaomi AIoT Router AX3600	248 користувачів	992 користувачів
Xiaomi Redmi AX5	128 користувачів	512 користувачів
Xiaomi Router 4A	64 користувачів	256 користувачів

Також можно зробити змішану мережу використувати два роутера Xiaomi AIoT Router AX3600 и два роутера Xiaomi Redmi AX5 тоді максимальне навантаження мережі 752 користувачів.

3. Стандарти безпеки

3.1 WPA

Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2) і Wi-Fi Protected Access 3 (WPA3)-це три програми сертифікації безпеки і безпеки, розроблені Альянсом Wi-Fi для захисту бездротових комп'ютерних мереж. Альянс визначив їх у відповідь на серйозні недоліки, які дослідники виявили в попередній системі, Wired Equivalent Privacy (WEP).

WPA (іноді званий проектом стандарту IEEE 802.11 i) став доступний в 2003 році. Альянс Wi-Fi задумав його як проміжну міру в очікуванні доступності більш безпечного і складного WPA2, який став доступний в 2004 році і є загальним скороченням для повного стандарту IEEE 802.11 i (або IEEE 802.11 i-2004).

У січні 2018 року Wi-Fi Alliance оголосила про випуск WPA 3 з декількома поліпшеннями безпеки в порівнянні з WPA2.

Альянс Wi-Fi мав намір використовувати WPA як проміжний захід, щоб замінити WEP до появи повного стандарту IEEE 802.11 i. WPA може бути реалізований за допомогою оновлення вбудованого ПЗ на інтерфейсних картах бездротової мережі, призначених для WEP, які почали поставлятися ще в 1999 році. Однак, оскільки зміни, необхідні в точках бездротового доступу (APS), були більшими, ніж зміни, необхідні на мережевих картах, більшість точок доступу до 2003 року не могли бути оновлені для підтримки WPA.

Протокол WPA реалізує більшу частину стандарту IEEE 802.11 i. зокрема, для WPA був прийнятий Протокол цілісності тимчасових ключів (TKIP). WEP використовував 64-розрядний або 128-розрядний ключ шифрування, який повинен бути введений вручну на бездротових точках доступу і пристроях і не змінюється. TKIP використовує ключ для кожного пакета, що означає, що він динамічно генерує новий 128-бітний ключ для

кожного пакета і, таким чином, запобігає типам атак, які скомпрометували WEP

WPA також включає перевірку цілісності повідомлень, яка призначена для запобігання зміни і повторної відправки пакетів даних зловмисником. Це замінює циклічну перевірку надмірності (CRC), яка використовувалася стандартом WEP. Основний недолік CRC полягав у тому, що він не забезпечував достатньо надійної гарантії цілісності даних для пакетів, які він обробляв для вирішення цих проблем існували добре перевірені коди аутентифікації повідомлень, але вони вимагали занадто багато обчислень для використання на старих мережевих картах. WPA використовує алгоритм перевірки цілісності повідомлень, який називається TKIP, для перевірки цілісності пакетів. TKIP набагато сильніше, ніж CRC, але не настільки сильний, як алгоритм, який використовується в WPA2. З тих пір дослідники виявили недолік у WPA, який спирався на старі слабкі місця в WEP і обмеження хеш-функції коду цілісності повідомлень, названої Michael, для вилучення ключового потоку з коротких пакетів для повторного введення і підміни.

3.2 **WPA2**

Протокол WPA2 - це оновлена версія WPA, яка використовує шифрування AES і довгі паролі для створення захищеної мережі. WPA2 має версії для особистого і корпоративного використання, що робить його ідеальним варіантом як для домашніх користувачів, так і для підприємств. Однак для роботи цього протоколу потрібно більше обчислювальних потужностей, тому, якщо у вас старий пристрій, то цей протокол може працювати на ньому повільно або взагалі не працювати.

Ратифікований у 2004 році. WPA2, який вимагає тестування і сертифікації Альянсом Wi-Fi, реалізує обов'язкові елементи стандарту IEEE 802.11 і. зокрема, він включає обов'язкову підтримку CCMP, режиму шифрування на основі AES. Сертифікація розпочалася у вересні 2004 року. З

13 березня 2006 року по 30 червня 2020 року сертифікація WPA2 була обов'язковою для всіх нових пристроїв, що мають торгову марку Wi-Fi.

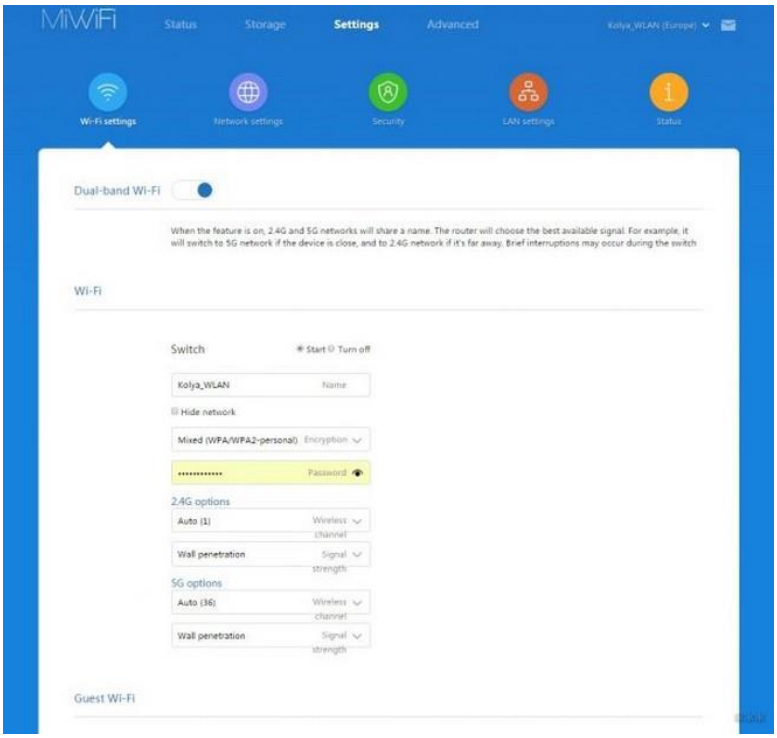


Рисунок 3.2.1 Настройка WPA2

3.3 WPA3

3.3.1 Основні відомості

У січні 2018 року Альянс Wi-Fi оголосив WPA3 як заміну WPA2.Сертифікація почалася в червні 2018 року.

Новий стандарт використовує еквівалентну 192-бітну криптографічну силу в режимі WPA3-Enterprise (AES-256 в режимі GCM з SHA-384 в якості HMAC) і як і раніше вимагає використання CCMP-128 (AES-128 в режимі CCM) в якості мінімального алгоритму шифрування в режимі WPA3-Personal.

Стандарт WPA3 також замінює обмін попередньо розділеним ключем (PSK) з одночасною аутентифікацією обміну рівними (SAE), метод, спочатку введений з IEEE 802.11 s, що призводить до більш безпечного початкового обміну ключами в особистому режимі і прямої секретності. Альянс Wi-Fi також стверджує, що WPA3 пом'якшить проблеми безпеки, пов'язані зі

слабкими паролями, і спростить процес налаштування пристроїв без інтерфейсу дисплея.

Захист кадрів управління, як зазначено в поправці IEEE 802.11 w, також забезпечується специфікаціями WPA3.

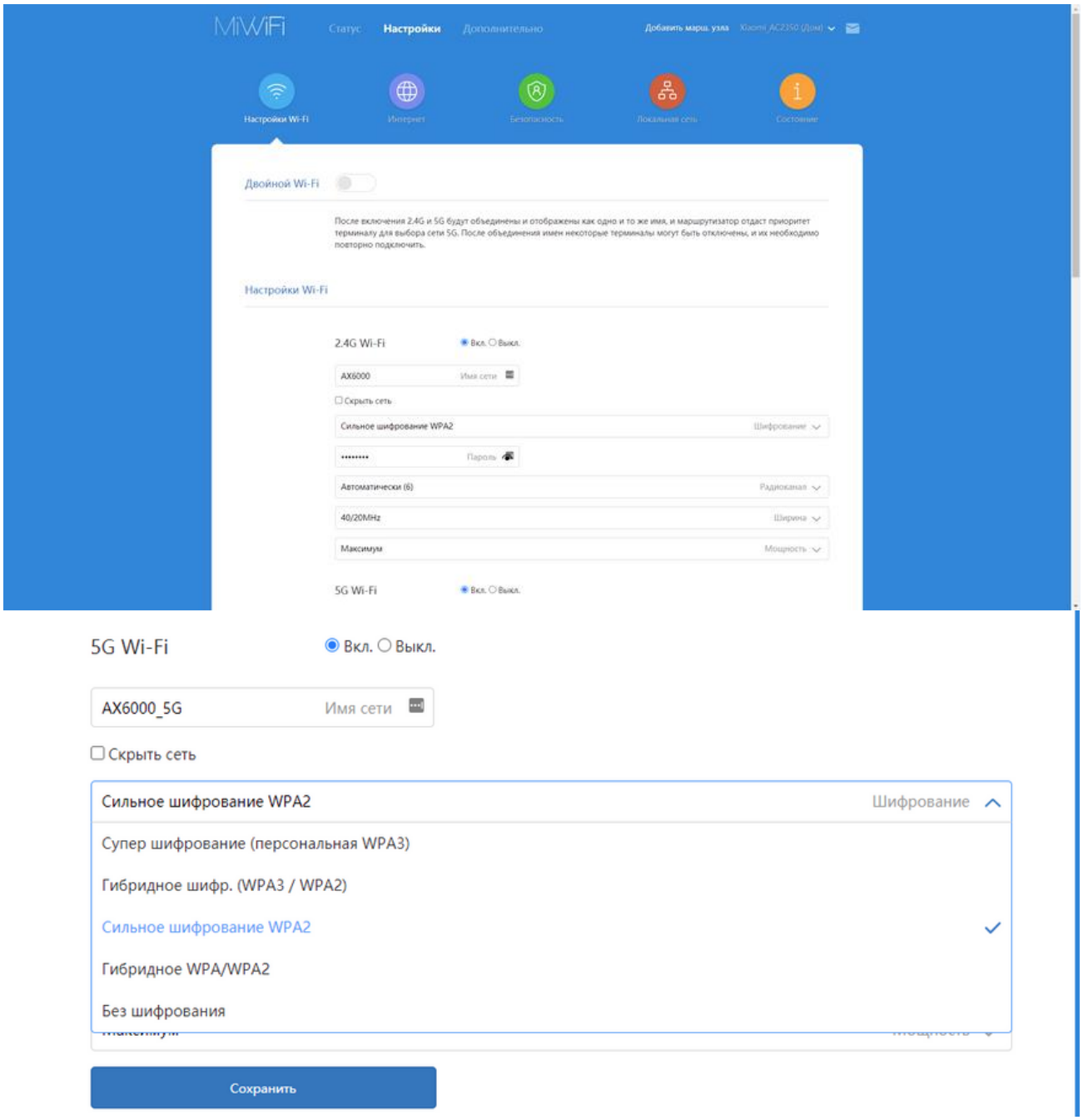


Рисунок 3.3.1 Настройка WPA2

3.3.2 Слабкий пароль

Попередньо розділені Ключі WPA і WPA2 залишаються вразливими для злому паролів, якщо користувачі покладаються на слабкий пароль або парольну фразу. Хеші парольних фраз WPA висіваються з імені SSID і його довжини; райдужні таблиці існують для 1000 кращих мережевих SSID і безлічі поширених паролів, що вимагають тільки швидкого пошуку для прискорення злому WPA-PSK.

Грубе примусове використання простих паролів може бути зроблено за допомогою пакета Aircrack, починаючи з чотиристороннього рукостискання аутентифікації, яким обмінюються під час асоціації або періодичної повторної аутентифікації.

WPA3 замінює криптографічні протоколи, схильні до автономного аналізу, протоколами, які вимагають взаємодії з інфраструктурою для кожного вгаданого пароля, імовірно встановлюючи тимчасові обмеження на кількість припущень. однак конструктивні недоліки в WPA3 дозволяють зловмисникам правдоподібно запускати атаки грубої сили

3.3.3 Відсутність прямої секретності

WPA і WPA2 не забезпечують прямої секретності, а це означає, що, як тільки зловмисник виявить попередньо загальний ключ, він потенційно може розшифрувати всі пакети, зашифровані за допомогою цього PSK, переданого в майбутньому і навіть в минулому, які можуть бути пасивно і мовчки зібрані зловмисником. Це також означає, що зловмисник може непомітно перехоплювати і розшифровувати чужі пакети, якщо точка доступу, захищена WPA, надається безкоштовно в громадському місці, оскільки її пароль зазвичай передається всім, хто знаходиться в цьому місці. Іншими словами, WPA захищає лише від зловмисників, які не мають доступу до пароля. Через це безпечніше використовувати безпеку транспортного рівня (TLS) або щось подібне для передачі будь-яких конфіденційних даних. Однак, починаючи з WPA3, ця проблема була вирішена.

3.3.4 Підміна і розшифровка пакетів WPA

Мати Ванхоф і Френк П'єсенс значно покращили атаки WPA-TKIP Еріка Тьюса і Мартіна Бека. вони продемонстрували, як вводити довільну кількість пакетів, причому кожен пакет містить не більше 112 байт корисного навантаження. Це було продемонстровано впровадженням сканера портів, який може бути виконаний проти будь-якого клієнта з використанням WPA-TKIP. Крім того, вони показали, як розшифрувати довільні пакети, відправлені клієнту. Вони згадали, що це може бути використано для захоплення TCP-з'єднання, дозволяючи зловмиснику вводити шкідливий JavaScript, коли жертва відвідує веб-сайт. На відміну від цього, атака Бека-Тьюса могла розшифровувати тільки короткі пакети з в основному відомим вмістом, такі як повідомлення ARP, і дозволяла вводити тільки від 3 до 7 пакетів не більше 28 байт. Атака Beck-Tews також вимагає включення якості обслуговування (як визначено в стандарті 802.11 e), в той час як атака Vanhoef-Piessens цього не робить. Жодна з атак не призводить до відновлення загального ключа сеансу між клієнтом і точкою доступу. Автори стверджують, що використання короткого інтервалу відновлення може запобігти деяким атакам, але не всім, і настійно рекомендують перейти з TKIP на CCMP на основі AES.

Халворсен та інші показують, як змінити атаку Бека-Тьюса, щоб дозволити ін'єкцію від 3 до 7 пакетів розміром не більше 596 байт. недоліком є те, що їх атака вимагає значно більше часу для виконання: приблизно 18 хвилин і 25 секунд. В іншій роботі Ванхоеф і П'єсенс показали, що, коли WPA використовується для шифрування широкомовних пакетів, їх початкова атака також може бути виконана це важливе розширення, оскільки значно більше мереж використовують WPA для захисту широкомовних пакетів, ніж для захисту одноадресних пакетів. Час виконання цієї атаки становить в середньому близько 7 хвилин у порівнянні з 14 хвилинами початкової атаки Ванхофа-П'єсенса і Бека-Тьюса.

Уразливості TKIP значні, оскільки WPA-TKIP раніше вважався надзвичайно безпечною комбінацією; дійсно, WPA-TKIP як і раніше є

варіантом конфігурації для широкого спектру пристроїв бездротової маршрутизації, що надаються багатьма постачальниками обладнання. Опитування, проведене в 2013 році, показало, що 71% як і раніше допускають використання TKIP, а 19% підтримують виключно TKIP.

3.3.5 Відновлення PIN-коду WPS

Більш серйозний недолік безпеки був виявлений в грудні 2011 року Стефаном Вьебеком, який впливає на Бездротові маршрутизатори з функцією Wi-Fi Protected Setup (WPS), незалежно від того, який метод шифрування вони використовують. Більшість останніх моделей мають цю функцію і включають її за замовчуванням. Багато виробників споживчих пристроїв Wi-Fi вжили заходів для усунення потенціалу вибору слабких парольних фраз, просуваючи альтернативні методи автоматичного створення і поширення надійних ключів, коли користувачі додають новий бездротовий адаптер або пристрій в мережу. Ці методи включають натискання кнопок на пристроях або введення 8-значного PIN-коду.

Альянс Wi-Fi стандартизував ці методи як захищену настройку Wi-Fi; однак широко реалізована функція PIN-коду призвела до появи нового серйозного недоліку безпеки. Цей недолік дозволяє віддаленому зловмиснику відновити PIN-код WPS і разом з ним пароль WPA/WPA2 маршрутизатора протягом декількох годин. користувачам настійно рекомендується відключити функцію WPS, хоча це може бути неможливо на деяких моделях маршрутизаторів. Крім того, PIN-код записаний на етикетці на більшості маршрутизаторів Wi-Fi з WPS і не може бути змінений в разі компрометації.

WPA3 вводить нову альтернативу для конфігурації пристроїв, які не мають достатніх можливостей інтерфейсу, дозволяючи довколишніх пристроїв служити адекватним інтерфейсом для цілей підготовки мережі, тим самим зменшуючи потребу в WPS.

3.3.6 MS-CHAPv2 і відсутність перевірки CN сервера AAA

У MS-CHAPv2 було виявлено кілька слабких місць, деякі з яких значно знижують складність атак грубої сили, що робить їх можливими за допомогою

сучасного обладнання. У 2012 році складність злому MS-CHAPv2 була зведена до злому одного ключа DES, роботи Моксі Марлінспайк і Маршу Рея. Моксі порадив: "підприємства, які залежать від властивостей взаємної аутентифікації MS-CHAPv2 для підключення до своїх серверів WPA2 Radius, повинні негайно почати перехід на щось інше".

Тунельні методи EAP з використанням TTLS або PEAP, які шифрують обмін MSCHAPv2, широко використовуються для захисту від використання цієї уразливості. Однак поширені клієнтські реалізації WPA2 на початку 2000-х років були схильні до неправильного Налаштування кінцевими користувачами або в деяких випадках (наприклад, Android) не мали доступного користувачеві способу правильного налаштування перевірки сертифіката CNS сервера AAA. Це розширило актуальність початкової слабкості в MSCHAPv2 в сценаріях атаки MiTM. згідно з більш суворими тестами відповідності WPA2, оголошеними поряд з WPA3, сертифіковане клієнтське програмне забезпечення повинно буде відповідати певній поведінці, пов'язаній з перевіркою сертифіката AAA.

3.3.7 Прогнозований Груповий часовий ключ (GTK)

У 2016 році було показано, що стандарти WPA і WPA2 містять небезпечний генератор випадкових чисел (ГСЧ). Дослідники показали, що, якщо постачальники реалізують запропонований ГСЧ, зловмисник може передбачити Груповий ключ (GTK), який повинен бути випадковим чином згенерований точкою доступу (AP). Крім того, вони показали, що володіння GTK дозволяє зловмиснику вводити будь-який трафік в мережу і дозволяє зловмиснику розшифровувати одноадресний інтернет-трафік, що передається по бездротовій мережі. Вони продемонстрували свою атаку на маршрутизатор Asus RT-AC51U, який використовує драйвери MediaTek out-of-tree, які самі генерують GTK, і показали, що GTK може бути відновлений протягом двох хвилин або менше. Аналогічним чином, вони продемонстрували Ключі, створені демонами Broadcom access, що працюють на VxWorks 5 і пізніших версіях, які можуть бути відновлені за чотири хвилини або менше, що впливає,

наприклад, на деякі версії Linksys WRT54G і деякі моделі Apple AirPort Extreme. Постачальники можуть захиститися від цієї атаки за допомогою захищеного ГСЧ. Таким чином, Hostapd, що працює на ядрах Linux, не вразливий до цієї атаки, і тому маршрутизатори, що працюють з типовими установками OpenWRT або LEDE, не виявляють цієї проблеми.

3.3.8 Атака KRACK

Основна стаття: KRACK

У жовтні 2017 року були опубліковані подробиці атаки KRACK (Key Reinstall Attack) на WPA2 вважається, що атака KRACK впливає на всі варіанти WPA і WPA2; однак наслідки для безпеки варіюються в залежності від реалізації, в залежності від того, як окремі розробники інтерпретували погано визначену частину стандарту. Виправлення програмного забезпечення можуть усунути вразливість, але доступні не для всіх пристроїв

ВИСНОВКИ

Під час виконання роботи було проведено огляд стандартів IEEE 802.11. Найкраще підходить стандарт Wi-Fi 802.11n тому що він підтримує діапазон 2.4 і 5 ГГц, також він сумісний з 802.11 a/b/g. Максимальна швидкість до 600 Мбіт/с.

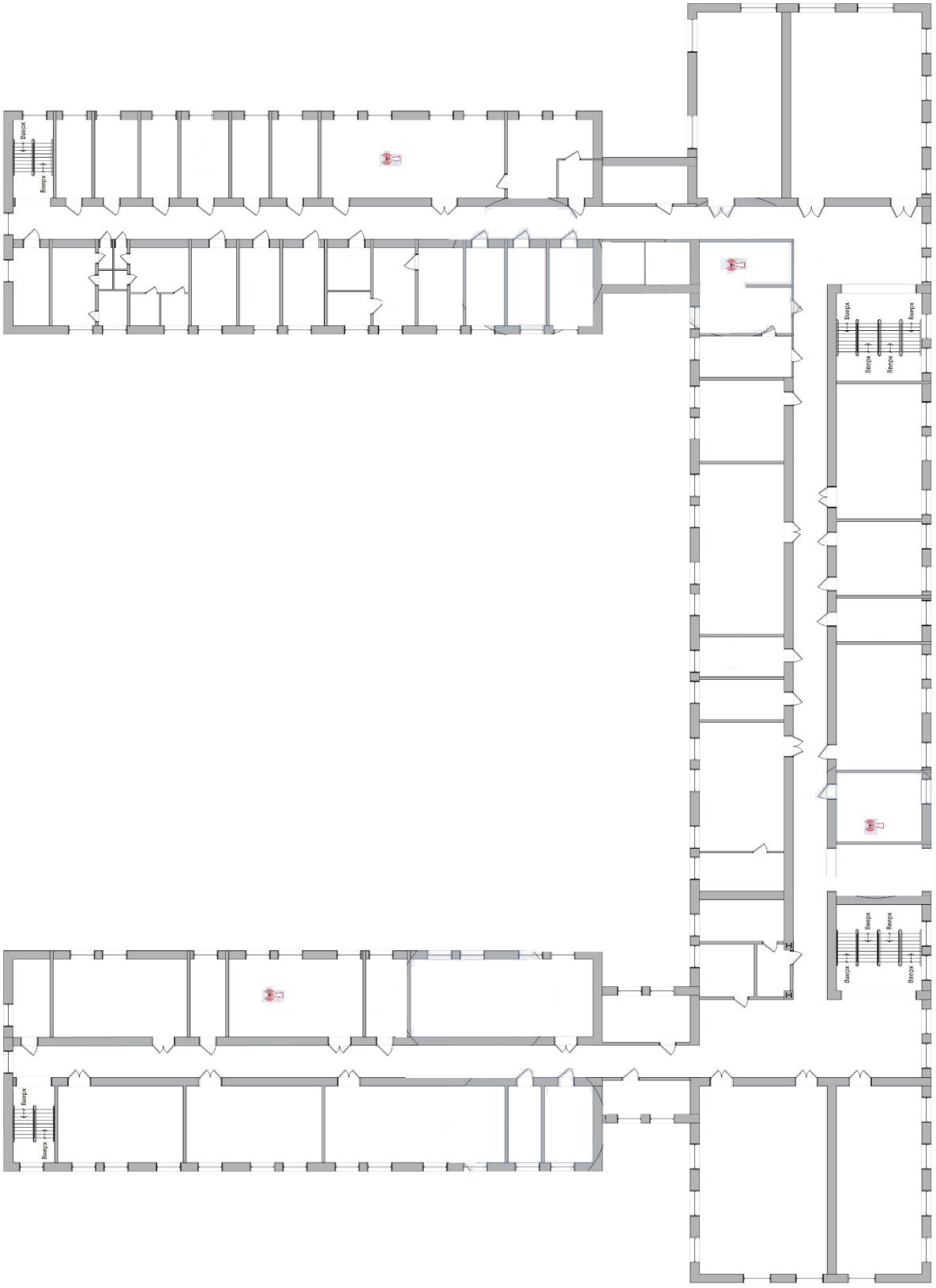
Згідно розрахунків найкращій варіант для оптимального покриття підприємства буде взяти два роутери AX5 та два роутери AX3600. В майбутньому можно зробити безшовне з'єднання wi-fi сети. Для більш конфортного користування. Виходячи з того, що площа приміщення 2072м^2 (534 м^2 ліве крило, 534 м^2 праве крило та 994м^2 центральна частина). Найкащій варіант встановлення роутерів наведенний на додатку 1.

СПИСОК ЛІТЕРАТУРИ

1. Getwifi [Електронний ресурс] — Режим доступу :https://www.getwifi.ru/p_router_ap.html
2. Controleng [Електронний ресурс] — Режим доступу: https://controleng.ru/besprovodny-e-tehnologii/putivoditel-iot-3-wi-fi/
3. Nag [Електронний ресурс] — Режим доступу: https://nag.ru/articles/reviews/104595/obzor-tehnologii-wi-fi.html
4. Comprice [Електронний ресурс] — Режим доступу: http://www.comprice.ru/articles/detail.php?ID=225105
5. Mi [Електронний ресурс] — Режим доступу : https://www.mi.com/global/mi-aiot-router-ax3600/
6. Wiki [Електронний ресурс] — Режим доступу: https://uk.wikipedia.org/wiki/IEEE_802.11
7. Awifi [Електронний ресурс] — Режим доступу : http:// awifi.ru/chto-takoe-wi-fi-3/
8. Wiki [Електронний ресурс] — Режим доступу: https://en.wikipedia.org/wiki/IEEE_802.11n-2009
9. Wiki [Електронний ресурс] — Режим доступу: https://en.wikipedia.org/wiki/IEEE_802.11a-1999
10. Nag [Електронний ресурс] — Режим доступу : https://nag.ru/material/35534
11. Ixbt [Електронний ресурс] — Режим доступу: https://www.ixbt.com/comm/wlan.shtml
12. Wiki [Електронний ресурс] — Режим доступу: https://en.wikipedia.org/w/index.php?search=IEEE+802+n&title=Special%3ASearch&profile=advanced&fulltext=1&ns0=1
13. Habr [Електронний ресурс] — Режим доступу: https://habr.com/ru/post/501266/

14. Wiki [Електронний ресурс] — Режим доступу: https://en.wikipedia.org/wiki/IEEE_802.11g-2003
15. Network [Електронний ресурс] — Режим доступу: http://network.xsp.ru/5_4.php
16. Xiaomi [Електронний ресурс] — Режим доступу: https://www.xiaomi.ua/router-mi-wifi-router-4a-3005098/p22244/
17. Xiaomi [Електронний ресурс] — Режим доступу: https://www.xiaomi.ua/router-xiaomi-redmi-ax5-white/p35350/
18. Wiki [Електронний ресурс] — Режим доступу: https://en.wikipedia.org/wiki/IEEE_802.11b-1999
19. Xiaomi [Електронний ресурс] — Режим доступу: https://www.xiaomi.ua/marshrutizator-xiaomi-aiot-router-ax3600/p33262/ [
20. Wifi [Електронний ресурс] — Режим доступу : http://1234g.ru/wifi/standarty-wifi
21. Keenetic [Електронний ресурс] — Режим доступу: https://help.keenetic.com/hc/ru/articles/Wi-Fi-4-IEEE-802-11n-
22. Spbsut [Електронний ресурс] — Режим доступу: http://opds.spbsut.ru/data/_uploaded/mu/bspd/vlss19mu_bspd_prakt_802.pdf

ДОДАТОК 1


Вверх
Вверх
Вверх
Вверх
Вверх
Вверх
Вверх
Вверх
Вверх
Вверх