ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно- інтегрованих технологій, автоматизації, електроінженерії та радіоелектроніки
(повне найменування інституту, назва факультету)

Автоматика та телекомунікації
(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри

_____

_____
(підпис) (ініціали, прізвище)

"___"_____20_ р.

Випускна кваліфікаційна робота

магістра
(освітньо-кваліфікаційний рівень)

на тему «Дослідження та модернізація мережі безпроводового абонентського доступу комунального підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради» з урахуванням механізмів безпеки»

Виконав : студент 2 курсу, групи ТКРм-19
(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)

Тіссен О. С. _____
(прізвище та ініціали) (підпис)

Керівник к.т.н., доц., проф. каф. АТ Воропаєва В.Я. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Покровськ – 2020 р.

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно- інтегрованих технологій, автоматизації, електроінженерії та радіоелектроніки
(повне найменування інституту, назва факультету)

Автоматика та телекомунікації
(повна назва кафедри)

Захист відбувся_____
(дата)
з оцінкою _____
секретар ДЕК_____
(підпис)

Випускна кваліфікаційна робота

магістра
(освітньо-кваліфікаційний рівень)

на тему «Дослідження та модернізація мережі безпроводового абонентського доступу комунального підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради» з урахуванням механізмів безпеки»

Виконав студент групи ТКРм-19 Тіссен О. С.
(підпис, дата) (ініціали, прізвище)

Керівник к.т.н., доц., проф. каф. АТ Воропаєва В.Я.
(підпис, дата) (ініціали, прізвище)

Зав. каф. автоматики та телекомунікацій _____
(підпис, дата) (ініціали, прізвище)

Консультанти _____.
(підпис, дата) (ініціали, прізвище)

_____
(підпис, дата) (ініціали, прізвище)

_____
(підпис, дата) (ініціали, прізвище)

Нормоконтролер
_____
(підпис, дата) (ініціали, прізвище)

Покровськ – 2020 р.

ДВНЗ «Донецький національний технічний університет»

Факультет комп'ютерно- інтегрованих технологій, автоматизації електроінженерії та радіоелектроніки
Кафедра автоматика та телекомунікації
Освітній ступінь магістр
Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ:
Завідувач кафедри
_____ /_____/
"____" _____20___року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІАЦІЙНУ РОБОТУ СТУДЕНТУ

Тіссена Олександра Сергійовича
(прізвище, ім'я, по батькові)

1. Тема роботи «Дослідження та модернізація мережі безпроводового
«Дослідження та модернізація мережі безпроводового абонентського доступу комунального підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради» з урахуванням механізмів безпеки»

керівник роботи: к.т.н., доц., проф. каф. АТ Воропаєва В.Я.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом від "23" вересня 2019 року № 693
2. Строк подання студентом роботи _____
3. Вихідні дані до роботи: характеристика комунального підприємства, плани всіх амбулаторій, кількість користувачів мережею
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1) Аналіз та характеристика комунального підприємства для розробки проекту
2) Розбудова архітектури мережі безпроводового доступу
3) Побудова інформаційної моделі мережі та структурної схеми
4) Вибір точок доступу та їх кількість, модулювання зони покриття мережі
5) Моделювання радіопокриття для безпроводової мережі, що проектується
6) Дослідження механізмів безпеки безпроводової мережі
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
— плани будівель підприємства для проектування
— інформаційна модель мережі
— структурна схема
— модель радіопокриття безпроводової мережи
— модель зони покриття мережі

6. Консультанти розділів проекту (роботи)

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

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Проходження практики на підприємстві КП «ЦПМСД» Покровської міської ради	01.09.20-11.09.20	
2	Отримання статистичних даних та характеристики підприємства	12.09.20-25.09.20	
3	Порівняння та вибір необхідних технології та обладнання	26.09.20-09.10.20	
4	Розробка інформаційної моделі мережі та структурної та схеми	10.10.20-23.10.20	
5	Моделювання зони покриття мережі безпроводового доступу	24.10.20-06.11.20	
6	Аналіз середі у місці проектування мережі та моделювання радіопокриття мережі	07.11.20-20.11.20	
7	Дослідження механізмів безпеки безпроводових мереж	21.11.20-03.12.20	
8	Захист роботи	23.12.20	

Студент _____ **Тіссен О.С**
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ **Воропаєва В.Я.**
(підпис) (прізвище та ініціали)

Лист зауважень

Посада П.І.Б.	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Тіссен О.С. «Дослідження та модернізація мережі безпроводового абонентського доступу комунального підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради» з урахуванням механізмів безпеки» / Випускна кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 172 Телекомунікації та радіотехніка. – ДВНЗ ДонНТУ, Покровськ, 2020.

Робота містить 92 сторінка, складається з вступу, 5 розділів, висновків, переліка використаних джерел з 30 найменувань, 1 додаток, 38 рисунків, 16 таблиць.

Дипломна робота направлена на розробку мережі безпроводового доступу і, як наслідок, осучаснення КП «Центр первинної медико-санітарної допомоги» Покровської міської ради, також до уваги було взято питання безпеки мережі та було проведено дослідження механізмів безпеки безпроводових мереж. Зібрано необхідні статистичні та характеристичні дані підприємства КП «ЦПМСД». Розглянуто різні технології побудови безпроводових мереж, проведено аналіз статистичних даних та обрано технології, що будуть найбільш відповідними до вимог. Обрано необхідне обладнання. Розроблено модель безпроводової мережі для амбулаторій підприємства. Зроблено аналіз середи в місці проектування безпроводової мережі та розроблено моделювання радіопокриття безпроводової мережі, що проектується. Проведено дослідження механізмів безпеки безпроводових мереж.

Ключові слова: БЕЗПРОВОДОВА МЕРЕЖА, ПРОПУСКНА ЗДАТНІСТЬ, ТОЧКА ДОСТУПУ, ПРОЕКТУВАННЯ, НАВАНТАЖЕННЯ, ТЕХНОЛОГІЯ, МОДЕЛЮВАННЯ, ОБЛАДНАННЯ, ТОПОЛОГІЯ, ПОКРИТТЯ, БЕЗПЕКА.

Список публікацій здобувача:

1. Тіссен О.С. «Розробка мережі безпроводового доступу комунального підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради» / Всеукраїнської науково-практичної конференції молодих учених аспірантів та студентів «Телекомунікації, автоматизація, комп'ютерно-інтегровані та інформаційні технології» (ТАК-2019), - Покровськ ДВНЗ «ДонНТУ», 28 листопада 2019 р.
2. Тіссен О.С. «Особливі функції мережевого сервісу в мережевих вузлах з підтримкою SDN» / Всеукраїнської науково-практичної конференції молодих учених аспірантів та студентів «Автоматизація, контроль та управління: пошук ідей та рішень» (АКУ-2020), - Покровськ ДВНЗ «ДонНТУ», 21 травня 2020 р.
3. Тіссен О.С. «Дослідження та модернізація мережі безпроводового абонентського доступу комунального підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради» з урахуванням механізмів безпеки» / Всеукраїнської науково-практичної конференції молодих учених аспірантів та студентів «Телекомунікації, автоматизація, комп'ютерно-інтегровані та інформаційні технології» (ТАК-2020), - Покровськ ДВНЗ «ДонНТУ», 25-26 листопада 2020 р.

ABSTRACT

Tissen Oleksandr «Research and modernization of the wireless subscribers access network of utility company «Primary Health Care Center» of the Pokrovsky city council, taking into account security mechanisms» / Final qualification work for the degree of "Master" in the specialty 172 Telecommunications and radio engeneering. - SHEI DonNTU, Pokrovsk, 2020.

The work contains 92 pages, consists of an introduction, 5 sections, conclusions, a list of sources used with 30 items, 1 addition, 38 pictures, 16 tables.

Thesis is aimed at developing a wireless access network and, as a result, modernization of KP "Primary Health Care Center" of the Pokrovsky City Council, also took into account network security and conducted a study of security mechanisms of wireless networks. Necessary statistical and characteristic data of the enterprise KP "CPMSD" are collected. Various technologies of construction of wireless networks are considered, the analysis of statistical data is carried out and the technologies which will be the most corresponding to requirements are chosen. The necessary equipment has been selected. A model of a wireless network for outpatient clinics of the enterprise has been developed. The analysis of the environment in the place of designing the wireless network is made and the modeling of the radio coverage of the projected wireless network is developed. A study of security mechanisms of wireless networks.

Keywords: WIRELESS NETWORK, CAPACITY, ACCESS POINT, ENGINEERING, LOADING, TECHNOLOGY, MODELING, TOPOLOGY, COVERING, SECURITY.

List of applicant's publications:

1. Tissen Oleksandr «Development of a wireless access network of the utility company" Primary Health Care Center "Pokrovsky City Council» / All-Ukrainian scientific-practical conference of young graduate students and students «Telecommunications, automation, computer-integrated and information technology» (TAC-2019), - Pokrovsk SHEI «DonNTU», November 28, 2019.

2. Tissen Oleksandr «Special functions of network service in network nodes with SDN support» / All-Ukrainian scientific-practical conference of young graduate students and students «Automation, control and management: search for ideas and solutions» (ACM-2020), - Pokrovsk SHEI «DonNTU», May 21 2020

3. Tissen Oleksandr «Research and modernization of the wireless subscribers access network of utility company «Primary Health Care Center» of the Pokrovsky city council, taking into account security mechanisms» / All-Ukrainian scientific-practical conference of young graduate students and students «Telecommunications, automation, computer-integrated and information technologies» (TAC-2020), - Pokrovsk SHEI «DonNTU», November 25-26, 2020

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ГНН – година найбільшого навантаження;

КП – комунальне підприємство;

ПК – персональний комп'ютер

ТД – точка доступу;

ЦПМСД – Центр первинної медико-санітарної допомоги.

ВСТУП

У наш час телекомунікаційні технології розвиваються дуже швидко. Зараз нам дуже складно уявити своє життя без доступу до мережі інтернет, більшість з нас хоча б один раз на день заходить до різноманітних соціальних мереж з різних причин та ціле, будь-то месенджери для текстового, голосового або відео спілкування, чи розважальні соцмережі для проведення свого дозвілля. За статистикою за 2018 рік близько сімдесяти відсотків відвідувачів для доступу до соціальних мереж використовують смартфони завдяки безпроводовому доступу до всесвітньої мережі інтернет. Адже, не тільки смартфони використовують для виходу до всесвітньої інтернет павутини. З кожним роком з’являється ще більше різної побутової техніки чи периферійних пристроїв які підтримують безпроводовий доступ до інтернет мережі, для можливості віддаленого доступу до них та користування ними без додаткових кабелів. Але дуже важливою частиною у проектуванні безпроводової мережі є питання механізмів безпеки, яке слід дослідити та обрати необхідну технологію забезпечення безпеки мережі.

Актуальність теми — розробка покриття для безпроводового доступу до інтернет мережі якою зможуть користуватися відвідувачі та працівники комунального підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради для особистих або робочих цілей, наприклад, консультації пацієнтів або відеоконференції з урахуванням та дослідженням механізмів безпеки.

Метою дипломного проекту є розробка мережі безпроводового доступу для особистого користування та для працівників для особистих або робочих цілей.

Щоб виконати роботу необхідно виконати **наступні задачі**:

— охарактеризувати комунальні підприємства «Центра первинної медико-санітарної допомоги» Покровської міської ради

— зробити характеристику наданих послуг для мережі

— розрахувати навантаження для кожної будівлі у підприємстві

— визначити необхідну топологію для побудови безпроводового доступу

— розробити інформаційну модель мережі та функціональну схему

— визначити відповідні до розробленої мережі точки доступу та їх необхідну кількість для кожної побудови

— проаналізувати середу безпроводових мереж у середі проектування

— дослідити механізми безпеки для надання необхідного захисту для безпроводової інтернет-мережі

В якості **об'єкту дослідження** для виконання проекту буде виступати комунальне підприємство «Центр первинної медико-санітарної допомоги» Покровської міської ради (м. Покровськ, с. Шевченко, м. Родинське). Для підприємства буде розроблена безпроводова мережа, яка надасть вільний доступ до інтернет мережі для усіх відвідувачів та працівників.

Предметом дослідження є створення доступу безпроводової мережі для доступу в інтернет та забезпечення мережі надійним захистом.

Методами дослідження виступає розрахунок навантаження на мережу, визначення необхідних технологій та кількість і вид обладнання. Моделювання радіопокриття та забезпечення мережі механізмами безпеки.

Структура та обсяг роботи. Дипломна робота обсягом 92 машинописних сторінки, складається з вступу, п'яти розділів, висновків, переліка використаних джерел, що складається з 30 найменувань. Робота містить 38 рисунків, 16 таблиць, 1 додаток.

1 АНАЛІЗ ОБ’ЄКТУ ПРОЕКТУВАННЯ, ПОСТАНОВА ЗАДАЧІ

1.1 Характеристика та опис об’єкту.

У наш час тяжко уявити своє життя без доступу до інтернет мережі. Не лише розваги являють собою інтернет, багато людей використовують, наприклад, для сплати комунальних послуг або запису на будь-який прийом. Немало молоді зараз працюють через інтернет та їм потрібен постійний доступ до мережі, навіть коли вони виходять з дому. Людині може знадобиться вихід до мережі у будь-який момент, чи то для зв’язку з рідними або близькими, чи для невідкладної відповіді по роботі. І саме в такі моменти на допомогу громадянам приходять у допомогу безпроводові мережі доступу до інтернету. Звичайно, у нашій країні є покриття GSM та вже майже у кожному місті є навіть LTE, але воно недостатньо якісне та стабільне і у деяких місцях багатого скупчення людей буває важко навіть надіслати текстове повідомлення у відповідному додатку (месенджері). Звичайно, це не дуже вагомі перешкоди, але коли людині потрібен доступ для мережі, щоб працювати через ноутбук, наприклад, здійснення відео-конференцій або надсилання деяких документів, які можуть багато важити, де потрібне якісне з’єднання на гарній швидкості. І саме в такі моменти на допомогу приходять вільні мережі безпроводового доступу, але найчастіше їх можна знайти у кафе чи торгово-розважальних центрах, хоча люди тратять багато часу у державних закладах та, нажаль, в таких місцях Wi-Fi можна знайти у дуже рідких виключеннях. У попередніх дослідженнях було розглянуто та розроблено мережу безпроводового доступу для комунальні підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради [1].

У попередніх дослідженнях було розроблено безпроводові мережі для кожної з амбулаторій, які входять до комунального підприємства Покровської міської ради, яка включає до себе сім центрів первинної медико-санітарної допомоги, п’ять з яких розміщуються у місті Покровськ, а інші у сусідніх населених пунктах: місті Родинське та селі Шевченко.

Перша амбулаторія «ЦПМСД» знаходиться у місті Покровськ за адресою вулиця Маршала Москаленко, будинок 161, вона виступає головною амбулаторією з чотирьох поверхів, та яку в середньому відвідує 500 чоловік на добу, з яких десь близько 250 користуються Wi-Fi мережею і з попередніх досліджень потрібна мережа з сумарним навантаженням 62 Мбіт/с. Наразі амбулаторія має на кожному поверсі 16-ти портові некеровані комутатори, які підключені кабелем та оптоволоконне підключення зі швидкістю 100 Мбіт/с, де провайдером виступає «АЛЬТАІР».

Для даної амбулаторії було розроблено наступну модель покриття безпроводового доступу до мережі інтернет:

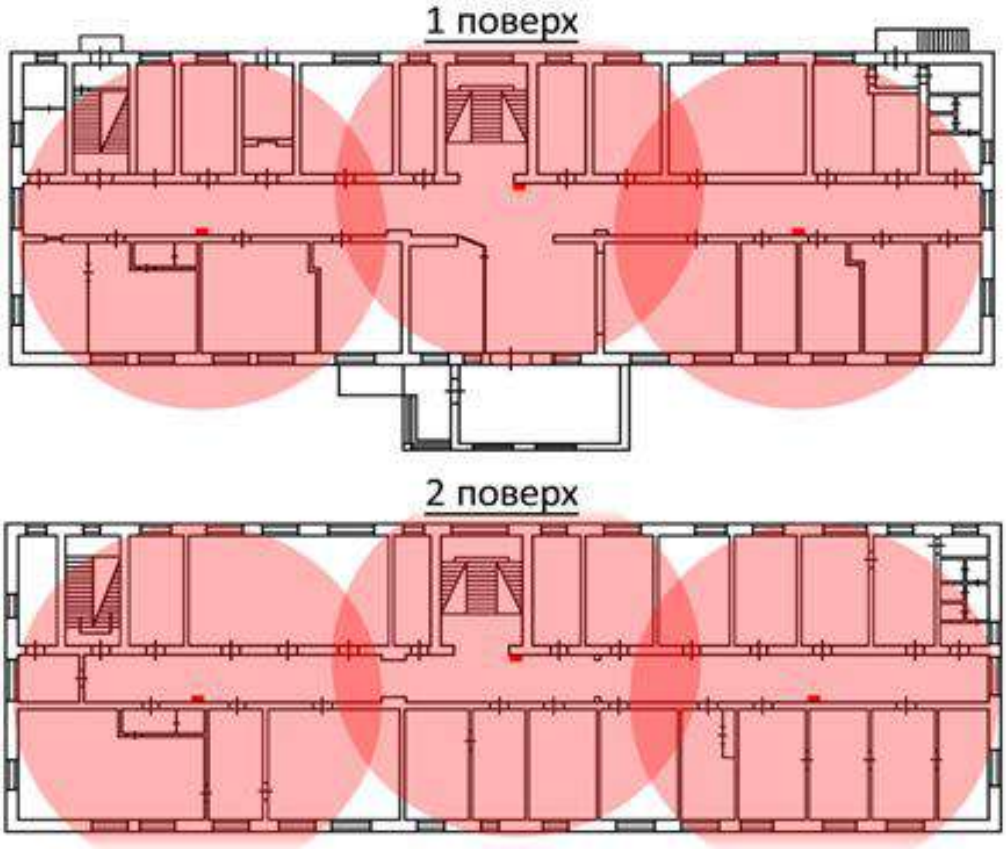


Рисунок 1.1 — Плани всіх поверхів Амбулаторії №1

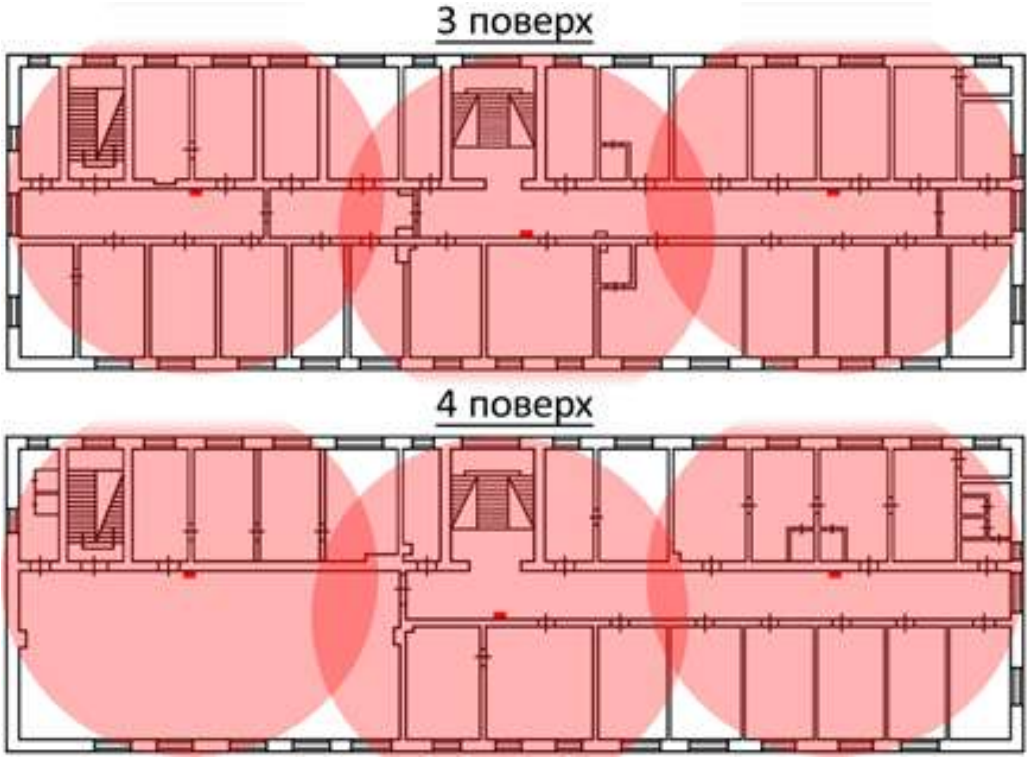


Рисунок 1.1 — Плани всіх поверхів Амбулаторії №1

Друга амбулаторія «ЦПМСД» знаходиться у місті Покровськ за адресою вулиця Лізи Чайкіної, будинок 49. В середньому її відвідує приблизно 80 чоловік на добу, з яких десь близько 50 користуються Wi-Fi мережею і з попередніх досліджень потрібна мережа з сумарним навантаженням 11 Мбіт/с. Це одноповерхова будівля, де встановлено некерований 8-ми портовий комутатор та точка доступу «MikroTik hEX RB750Gr3». Доступ до інтернет-мережі здійснює оптоволоконне підключення з пропускною здатністю 50 Мбіт/с, де провайдером виступає «АЛЬТАІР».

Для даної амбулаторії мною було розроблено наступну модель покриття безпроводового доступу до мережі інтернет:

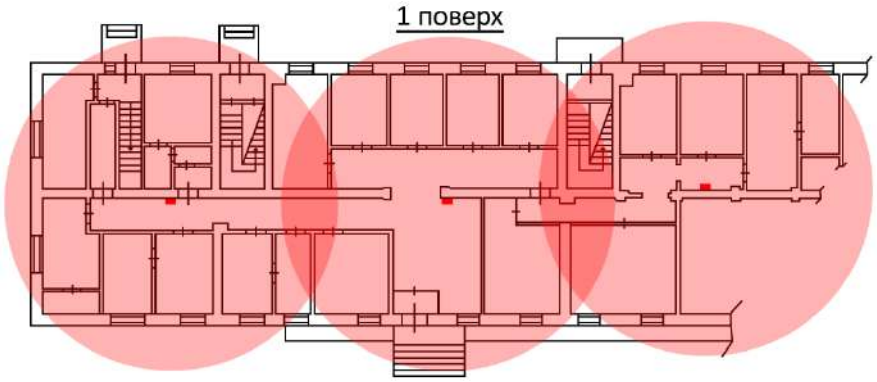


Рисунок 1.2 — План Амбулаторії №2

Амбулаторія №3 «ЦПМСД» знаходиться у місті Покровськ за адресою мікрорайон «Шахтарський», будинок 26-в/г. В середньому її відвідує приблизно 170 чоловік на добу, з яких десь близько 80 користуються Wi-Fi мережею і з попередніх досліджень потрібна мережа з сумарним навантаженням 22 Мбіт/с. Це одноповерхова будівля, де встановлено некерований 16-ти портовий комутатор та точка доступу «MikroTik hEX RB750Gr3». Доступ до інтернет-мережі здійснює оптоволоконне підключення з пропускною здатністю 50 Мбіт/с, де провайдером виступає «АЛЬТАІР».

Для даної амбулаторії мною було розроблено наступну модель покриття безпроводового доступу до мережі інтернет:

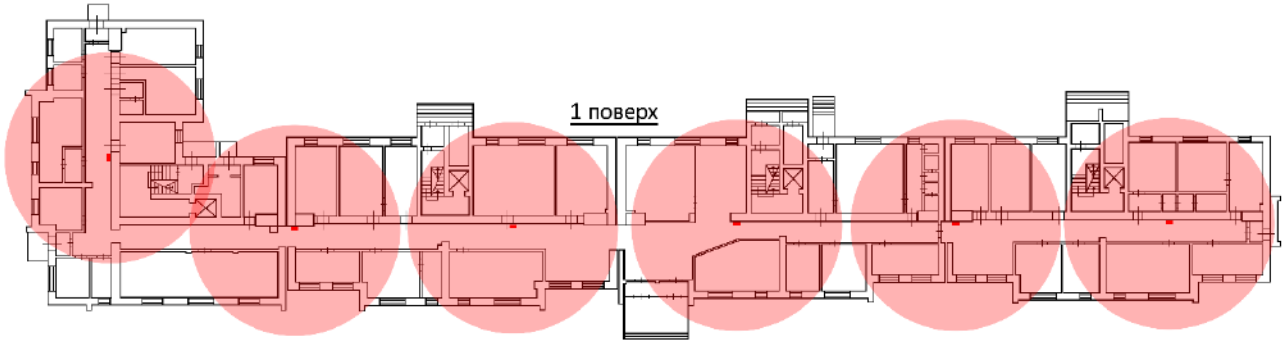


Рисунок 1.3 — План Амбулаторії №3

Амбулаторія №4 «ЦПМСД» знаходиться у місті Родинське за адресою вулиця Запорізька, будинок 5-а. В середньому її відвідує приблизно 90 чоловік на добу, з яких десь близько 45 користуються Wi-Fi мережею і з попередніх досліджень потрібна мережа з сумарним навантаженням 11 Мбіт/с. Це одноповерхова будівля, де встановлено некерований 16-ти портовий комутатор та точка доступу «MikroTik hEX RB750Gr3». Доступ до інтернет-мережі здійснює оптоволоконне підключення з пропускною здатністю 50 Мбіт/с, де провайдером виступає «Вірус.нет».

Для даної амбулаторії мною було розроблено наступну модель покриття безпроводового доступу до мережі інтернет:

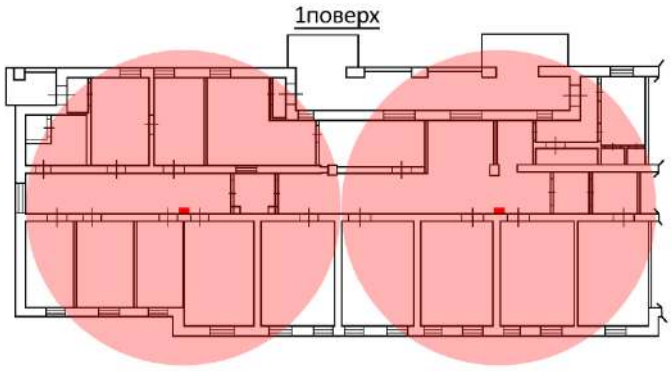


Рисунок 1.4 — План Амбулаторії №4

Амбулаторія №5 «ЦПМСД» знаходиться у селі Шевченко за адресою вулиця Центральна, будинок 1. В середньому її відвідує приблизно 35 чоловік на добу, з яких десь близько 20 користуються Wi-Fi мережею і з попередніх досліджень потрібна мережа з сумарним навантаженням 4 Мбіт/с. Це одноповерхова будівля, де доступ до інтернет-мережі здійснює 3G модем з пропускною здатністю 2-3 Мбіт/с та наданням телекомунікаційних послуг виступає «Водафон».

Для даної амбулаторії мною було розроблено наступну модель покриття безпроводового доступу до мережі інтернет:

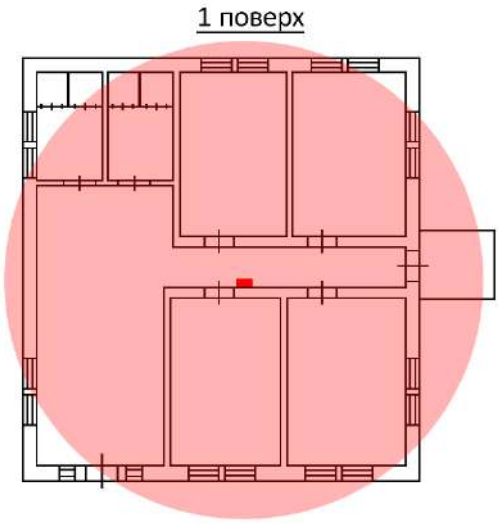


Рисунок 1.5 — План Амбулаторії №5

Амбулаторія №6 «ЦПМСД» знаходиться у місті Покровськ за адресою вулиця Степана Бовкуна, будинок 20. В середньому її відвідує приблизно 80 чоловік на добу, з яких десь близько 40 користуються Wi-Fi мережею і з попередніх досліджень потрібна мережа з сумарним навантаженням 11 Мбіт/с. Це одноповерхова будівля, де встановлено некерований 8-ти портовий комутатор та точка доступу «MikroTik hEX RB750Gr3». Доступ до інтернет-

мережі здійснює оптоволоконне підключення з пропускною здатністю 50 Мбіт/с, де провайдером виступає «АЛЬТАІР».

Для даної амбулаторії мною було розроблено наступну модель покриття безпроводового доступу до мережі інтернет:

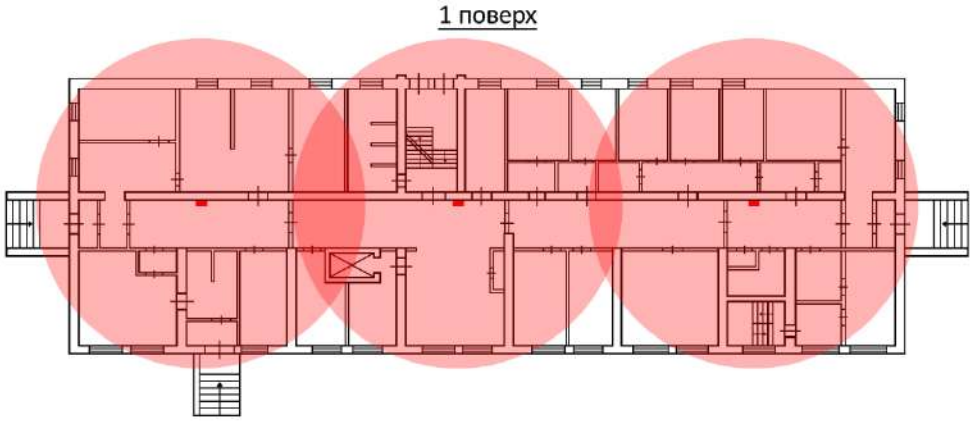


Рисунок 1.6 — План Амбулаторії №6

Амбулаторія №10 «ЦПМСД» знаходиться у місті Покровськ за адресою вулиця Захисників України, будинок 33. В середньому її відвідує приблизно 80 чоловік на добу, з яких десь близько 30 користуються Wi-Fi мережею і з попередніх досліджень потрібна мережа з сумарним навантаженням 7 Мбіт/с. Це одноповерхова будівля, де встановлено некерований 16-ти портовий комутатор та точка доступу «MikroTik hEX RB750Gr3». Доступ до інтернет-мережі здійснює оптоволоконне підключення з пропускною здатністю 50 Мбіт/с, де провайдером виступає «АЛЬТАІР».

Для даної амбулаторії мною було розроблено наступну модель покриття безпроводового доступу до мережі інтернет:

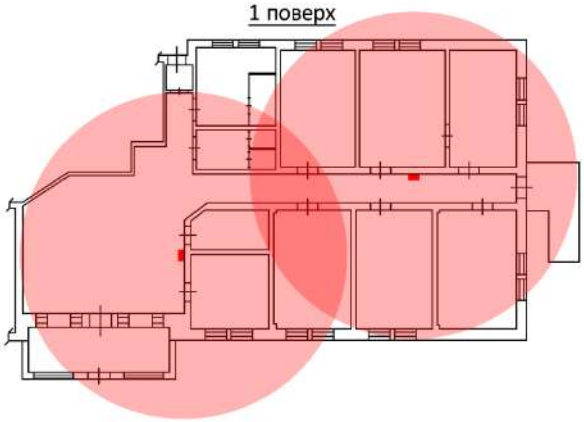
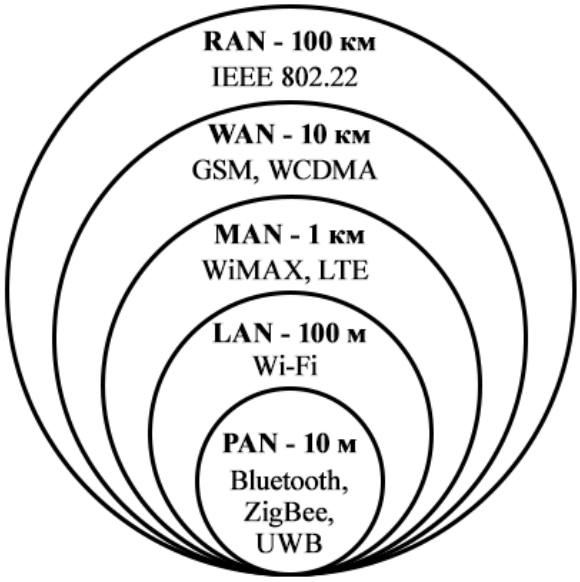


Рисунок 1.7 — План Амбулаторії №10

1.2 Типи безпроводових мереж та стандарти.

Безпроводові мережі створені для того, щоб забезпечити взаємодію між користувачами різноманітних серверів або баз даних. Підключення може здійснюватися декількома способами, такими як: Wi-Fi, Bluetooth та WiMax. Проводові та безпроводові мережі класифікуються за однаковими ознаками:

— Personal Area Network (PAN) — з’єднання між об’єктами, які знаходяться на невеликій відстані друг від друга, наприклад, мобільні телефони через технологію Bluetooth.
— Local Area Network (LAN) — з’єднання у межах однієї будівлі (Wi-Fi).
— Metropolitan Area Network (MAN) — з’єднання у межах одного міста (LTE).
— Wide Area Network (WAN) — глобальний вихід до мережі інтернет (GSM, WCDMA).



PAN — персональні мережі
IEEE 802.15.1 Bluetooth — 1 Мбіт/с
IEEE 802.15.3 UWB — 480 Мбіт/с
IEEE 802.15.4 ZigBee — 250 Кбіт/с

LAN — локальні мережі
IEEE 802.11 Wi-Fi — 1 Гбіт/с

MAN — міські мережі
IEEE 802.16 WiMAX — 145(DL)/138(UL) Мбіт/с
LTE — 300(DL)/75(UL) Мбіт/с

WAN — глобальні мережі
GSM, WCDMA — до 2 Мбіт/с

RAN — регіональні мережі
IEEE 802.22 — до 23 Мбіт/с

Рисунок 1.8 — Класифікація безпроводових мереж.

Головною специфікацією безпроводової мережи є протокол 802.11, якій поділяється на 6 поколінь: 802.11a/b/g/n/ac та новий стандарт 802.11ax. Попередні п’ять стандартів були розглянуті у попередніх дослідженнях, але на той час стандарт 802.11ax ще не був введений для загального користування у нашій країні [2].

IEEE 802.11ax (або Wi-Fi 6) — це новітній стандарт Wi-Fi, який здатен вирішити проблему з постійним зростанням кількості пристроїв, які використовують підключення до безпроводової мережі. Наразі у світі нараховується приблизно 15 мільярдів пристроїв, а через рік прогнозується, що ця кількість зросте понад 20 мільярдів. І саме новий стандарт 802.11ax повинен забезпечити користувачам швидке та стабільне безпроводове інтернет-покриття [3]. У порівнянні з попереднім стандартом 802.11ac, новий стандарт пропонує наступне:

Таблиця 1.1 – Порівняння стандартів 802.11ac та 802.11ax

	Стандарт

	802.11ac	802.11ax
Дата релізу	2013 рік	2019 рік
Робоча частота	2.4 ГГц та 5 ГГц	2.4 ГГц та 5 ГГц, охоплюючи діапазон від 1 ГГц до 7 ГГц.
Кількість піднесучіх	234 (80 МГц)	1960 (160 МГц)
Швидкість кадрування	5/6	5\6
Біт/символ	Log2(256)	Log2(1024)
Швидкість на символ OFDM	3.6 мкс	13.6 мкс
1SS	433.3 Мбіт/с	1.2 Гбіт/с
4SS	1.74 Мбіт/с	4.8 Гбіт/с
8SS	NA	9.6 Гбіт/с

Виходячи з цього, порівнюючи обидві стандарти Wi-Fi 5 та Wi-Fi 6 можна зробити наступні висновки:

1. OFDMA працює не тільки на прийом, та ще й на передачу.
2. Розрахований на багато користувачів 8x8 MIMO на передачу.
3. Більш високий рівень модуляції — 1024-QAM.
4. Збільшена довжина символу OFDM, у чотири рази більш піднесучі.
5. Робота поза приміщень.
6. Просторовий перерозподіл і використання OBSS
7. Знижене енергоспоживання. [4]

1.3 Аналіз проблем, які слід розглянути.

У попередніх дослідженнях було розроблено безпроводову мережу, але ряд важливих питань не було розглянуто. Звертаючи увагу на те, що об’єктом проектування виступало комунальне підприємство з надання медичних послуг, то зараз, у період пандемії коронавірусу багато людей повинно чекати своєї

черги на вулиці, на свіжому повітрі, яким також може знадобитись підключення до безпроводової мережі. Розроблена модель мережі охоплювала лише абонентів всередині приміщень отже, люди, які знаходяться на вулиці можуть не мати доступу до Wi-Fi роутерів через велику відстань. Сьогодні постає актуальна задача модернізації мережі таким чином, щоб відвідувачі амбулаторій які знаходяться поза будівлі теж могли безперешкодно користуватися безпроводовою мережею доступу до інтернету.

Але це не всі аспекти, які слід розглянути. Необхідно зробити перерахунок навантаження трафіка, тому що це є ключовою необхідністю при проектуванні мережі. Перерахунок параметрів буде проводитися за тією ж методикою, що була використана в попередніх дослідженнях, але з коригуванням на те, що основне пікове навантаження буде здійснюватися на роутери, які знаходяться біля входу до лікарні та потрібна більша пропускна здатність. Окрім цього, звертаючи увагу на те, що було реалізовано новий стандарт безпроводових технологій, потрібно буде передивитись обладнання, яке було обрано для проектування мережі, та здійснити підбір більш відповідного обладнання.

Наступним кроком необхідно змоделювати радіочастотне планування. При проектуванні безпроводової мережі необхідно дотримуватися переліку наступних вимог:

1. Вибір типу мережі.
2. Щільність користувачів.
3. Вимоги до покриття та швидкості передачі даних.
4. Особливості клієнтських пристроїв.
5. Вимоги до безпеки мережі.

Набор цих вимог можуть бути виконані при допомоги керування наступних параметрів:

1. Діапазон частот 2.4 ГГц або 5 ГГц.

2. Використовувані канали для обраного діапазону.
3. Потужність передатчику.
4. Тип та коефіцієнт посилення антени.
5. Дозволені швидкості передачі даних.

Отже, розглянемо кожен з пунктів більш детально. У діапазоні 5 ГГц велика кількість непересічних каналів та велика пропускна здатність, але наразі невелика кількість пристроїв має підтримку цього діапазону частот. У діапазоні 2.4 ГГц мається лише три непересічних канали, це 1, 6 та 11. Відповідно частотне планування повинно бути зроблено з цим урахуванням. Не слід розміщувати поруч дві точки доступу, які будуть працювати на одному частотному діапазоні, це може призвести до високих значень сигнальних шумів. У місцях високої щільності користувачів, наприклад, саме у черзі біля входу до амбулаторії, можна встановити до трьох Wi-Fi роутерів для підвищення пропускної здатності мережі, котрі будуть працювати на різних каналах та не заважати один одному. Слід зауважити, що діапазон зони покриття у діапазоні 5 ГГц значно менш, ніж у діапазоні 2.4 ГГц.

Для мережі передачі даних необхідно визначити мінімальну швидкість передачі даних на кінцях зони покриття та робити планування мережі з урахуванням цих даних. Для однієї й теж будівлі може бути необхідна різна кількість точок доступу. Наприклад, якщо необхідно покрити зону зі швидкістю не нижче ніж 11 Мбіт/с, то вистачить 6 точок доступу, а якщо не нижче ніж 24 Мбіт/с, то необхідно встановити 12 точок доступу. Також, можна заборонити ряд швидкостей на контролері, наприклад з 1 до 11 Мбіт/с, та тоді на межах мережі швидкість буде не менш, ніж 11 Мбіт/с.

Якщо у мережі активно використовується голосові повідомлення, необхідно робити перекриття сусідніх точок доступу не менш, ніж 15-20 відсотків при рівні сигналу не нижче, ніж -67 дБм, це може забезпечити якісне з’єднання під час передачі голосових повідомлень. При цьому рекомендовані значення потужності точок доступу лежать у діапазоні 35-50 мВт. Для систем

позиціонування застосовується більш складний підхід к проектуванню мережі, так як за основу береться не оптимальне покриття мережі, а оптимальне розміщення точок доступу.

На точках доступу знаходяться антени, які позволяють збільшити довжину зв’язку, не підвищуючи потужності передавача точки доступу. Таким чином, якщо є задача покриття достатньо великого простору або довгого коридору з низькою щільністю користувачів, можна скористатися зовнішніми антенами з великим коефіцієнтом посилення, як односпрямованими, так і всеспрямованими. Слід враховувати, що необхідно робити розміщення точок доступу з тими умовами, що не рекомендується одночасно підключати до однієї точки доступу більше, ніж 25 клієнтів. У випадку великої щільності користувачів або вимог мережі до високої пропускної здатності, необхідно зменшувати потужність передавачів та більш щільно встановлювати точки доступу [5].

1.4 Урахування механізмів безпеки.

На відміну від проводових мереж, для підключення до безпроводових мережам не потрібно мати фізичний доступ до активного мережевого обладнання, але достатньо знаходись у межах покриття точки доступу та встановити з нею зв’язок. В деяких випадках мережа може виходити далеко за межи фізичного об’єкту та навіть якщо вона побудована з урахуванням межи рівня сигналу, використання потужних безпроводових точок та спрямованих антен дозволяє зловмиснику взаємодіяти з точкою доступу на значній відстані.

Коли зловмисник виявляє цікаву для нього безпроводову мережу, він може сконцентрувати увагу на необхідному каналі та зібрати увесь трафік цієї мережі. Як і у випадку з несанкціонованим підключенням, зловмисник має можливість аналізувати пакети, знаходячись на значній відстані від точки доступу. Існує багато різноманітних мережевих аналізаторів для WLAN. У

якості прикладу можна прикласти програми, так як AirMagnet Laptop, Wildpackets Aeropack, CommView for WiFi для операційних систем Windows та Ethereal, або Kismet для Linux. Для роботи мережевого аналізатора необхідно встановити до системи спеціальні драйвери мережевої карти, підтримуючі роботу в режимі моніторингу (HostAP, AirJack, Madwifi, IPW2200 для Linux). Драйвери для Windows, як правило входять до поставки мережевого аналізатору.

Специфіка безпроводової мережі WLAN та Wi-Fi робить її досить вразливою до атак, спрямованих на відказ в обслуговуванні. На якість зв'язку можуть позначитися погодні умови, незначна зміна розміщення антени, використання безпроводової мережі у сусідній будівлі або офісу. Як показує практика, надійних методів захисту від атак на відказ в обслуговуванні не існує. Цю особливість безпроводової мережі необхідно враховувати при плануванні, та не використовувати Wi-Fi при передачі трафіку з високими вимогами к доступності.

При розробці безпроводових мереж були враховані функції безпеки від несанкціонованого підключення. Першим з запропонованих стандартів захисту був WEP (Wired Equivalent Privacy), що використовує криптографічний алгоритм RC4 з статичним розподілом ключів шифрування для аутентифікації клієнтів, що підключаються до мережі та шифрування переданого трафіку. Однак, WEP не забезпечує належного рівня безпеки для захисту безпроводових мереж. Сучасна підсистема безпеки сімейства стандартів 802.11 представлена двома специфікаціями: WPA та 801.11i. Перша з них, як і WEP, здійснює для захисту трафіку алгоритм RC4, але з динамічною генерацією ключів шифрування. Пристрої, підтримуючи 802.11i, у якості алгоритму шифрування використовують AES. Обидва протоколи 802.11i та WPA для аутентифікації пристроїв можуть застосовувати як статично розподілений ключ, так і технологію 802.1X.

Рішення про впровадження безпроводової мережі WLAN та Wi-Fi, як і будь-які впровадження IT-технології, має супроводжуватися аналізом ризків, розробкою політики безпеки та інструкцій адміністраторів та користувачів по роботі з технологією, яка впроваджується. При розгортанні Wi-Fi у великій мережі слід ураховувати механізми централізованого керування налаштування точок доступу та клієнтських станцій. Оскільки вимоги до безпеки безпроводової мережи відрізняються від проводової, слід розрізняти ці мережі за допомогою між мережевого екрану. Бажано контролювати налаштування робочих станцій та точок доступу як за допомогою активних засобів так і за допомогою безпроводових систем виявлення атак. Останні можуть допомогти також вирішити проблему підключення несанкціонованих безпроводових пристроїв [6].

Проблеми безпеки також стосуються не тільки передачі інформації по радіоканал. Це глобальне питання пов’язане з працездатністю любої системи, а тім паче відкритої. Завжди є ймовірність того прослухати ефір, віддалено перехопити сигнал, зламати систему та провести анонімну атаку. Щоб уникнути несанкціоноване підключення розроблені і застосовуються методи шифрування інформації, застосовуються паролі для отримання доступу на підключення, забороняється транслювання імені точки доступу (SSID), ставиться фільтр на користувачів, що підключаються до мережі, та інші мери безпеки. Основну загрозу представляють собою:

— «Чужаки» або несанкціоновані пристрої, котрі отримали доступ до точки доступу в обхід засобів захисту.
— Нехарактерна природа підключення дозволяє мобільним пристроям автоматично підключатися до довіреної мережі. Таким чином для доступу до інформації зловмисник має можливість переключити користувача на свою точку доступу з подальшою атакою для пошуку вразливих місць у захисті.

— Вразливості пов’язані з конфігурацією мереж та підключаємих пристроїв. Ризик виникає під час використовування слабких механізмів захисту, простих паролів та т.п.
— Невірно налаштована точка доступу. Багато користувачів мережі залишають значення паролів, IP-адрес та інші налаштування у тому виді, у котрому вони були налаштовані з заводу. Зловмиснику не складає труднощів проникнути до захищеної зони, переналаштувати мережеве обладнання під себе та користуватися ресурсами мережи.
— Злом кріптозахисту мережі дозволяє використовувати всередині мережі інформацію, що передається. Для злому шифрування зараз не треба мати спеціальних знань або навичок. Можна знайти велику кількість програм скануючих та підбираючих захисні паролі.

Слід зазначити, що технології злома постійно модернізуються, постійно знаходяться нові засоби та варіанти атак. Також існує великий ризик витоку інформації дозволяючий дізнатися топологію мережі та варіанти підключення до неї.

1.5 Характеристики послуг та класифікація абонентів.

Мережа, що виступає об’єктом проектування у дипломній роботі має надавати доступ до інтернет-мережі. Інформаційну модель мережі можна зобразити наступним чином, як відображена на рисунку 1.9.

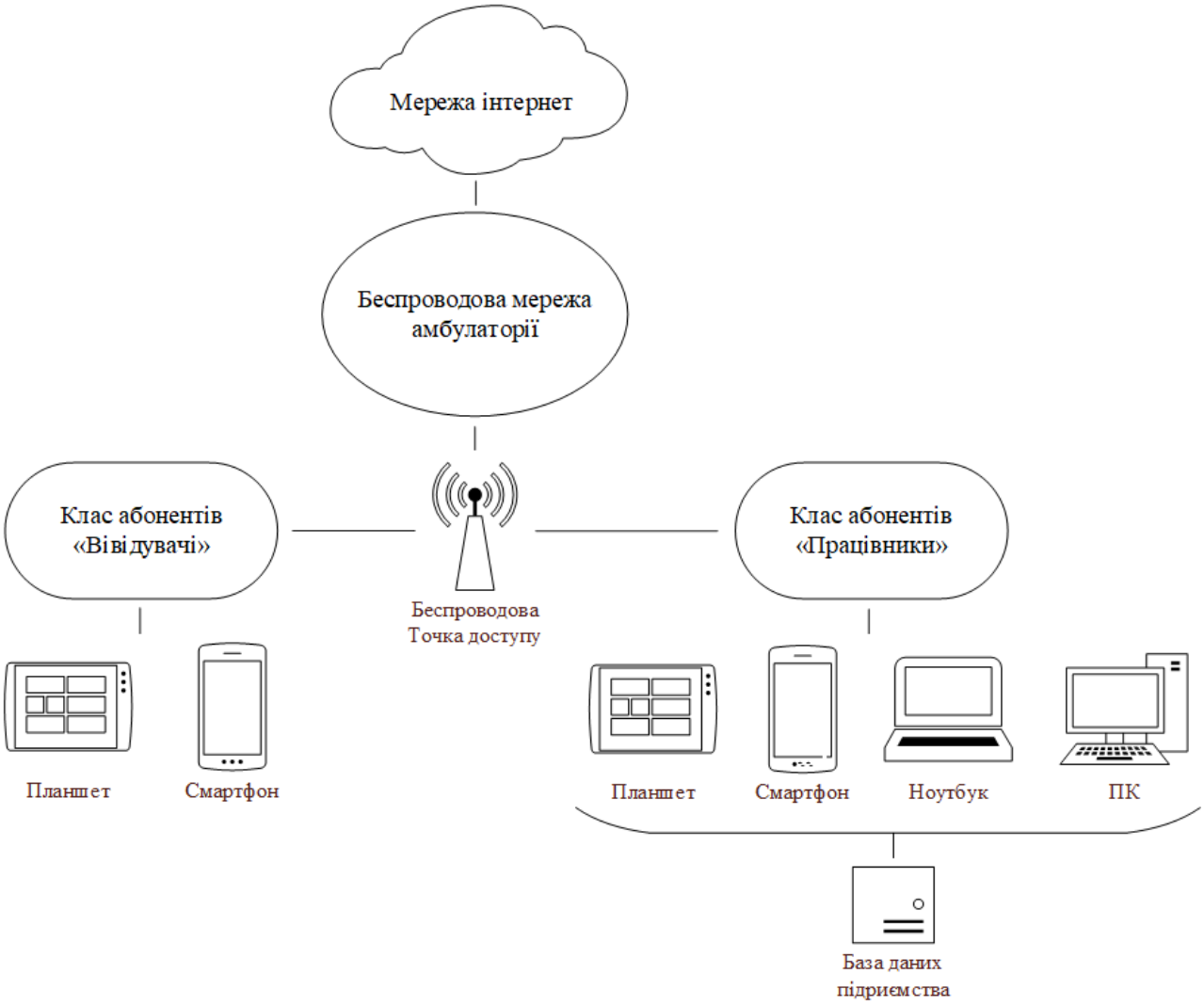


Рисунок 1.9 — Інформаційна модель мережі

Для коректного проектування інтернет мережі необхідно виділити типи абонентів та послуг. Це потрібно для того, щоб розроблена мережа була здатна задовольнити необхідні потреби, або не була занадто надлишковою, що може негативно скластися с фінансової точки зору.

Отже, виходячи з власних міркувань, можемо виділити наступні групи послуг:

— інтернет (web-серфінг);

— інтернет (електронна пошта, соц.мережі);

— інтернет телефонія, skype;

— відеоконференції;

— доступ до серверу.

Всі ці групи треба розподілити між класами абонентів. Всього ми можемо поділити на два класи, це працівники амбулаторій та їх відвідувачі. Співвідношення між класами та користувачами зведемо у таблиці 1.2.

Таблиця 1.2 – Групи абонентів та послуги

Тип послуги	Тип абонентів
Інтернет (web-серфінг)	Працівники та відвідувачі
Інтернет (електронна пошта, соц.мережі)	Працівники та відвідувачі
Інтернет телефонія, skype	Тільки працівники
Відеоконференції	Тільки працівники
Доступ до серверу	Працівники та відвідувачі

Наступним кроком потрібно визначити головні параметри кожного типу трафіку. Робити розрахунок будемо за параметрами, які надаються мережею у таблиці 1.3:

Таблиця 1.3 – Параметри трафіку інтерактивних служб

Тип	Послуга	Максимальна швидкість	Пачеч-ність	Тривалість сеансу зв'язку T_c, с	Частота викликів, ГНН
1	Інтернет (web-серфінг)	2,048 Мбіт/с	4	600	3
2	Інтернет (електронна пошта, соціальні мережі)	0,512 Мбіт/с	2	10	10
3	Інтернет телефонія, skype	0,128 Мбіт/с	1	180	3
4	Відеоконференції	1,024 Мбіт/с	1	240	1
5	Доступ до серверу	1,024 Мбіт/с	2	180	5

Параметри у таблиці є усередненими та були отримані завдяки власним міркуванням.

Висновки до розділу 1

Перша глава дипломного проекту включає в себе опис та характеристику об’єкту моделювання та модернізації мережі. Об’єктом модернізації мережі виступає комунальне підприємство «Центр первинної медико-санітарної допомоги» Покровської міської ради для якого у дипломному проекті бакалавра було розроблено мережу безпроводового доступу.

Було розглянуті класи безпроводових мереж та нові стандарти для безпроводових мереж і порівняні з попередніми стандартами. Серед інших недоліків необхідно переглянути та перерахувати розрахунки трафіку. Також потрібно змоделювати частотне планування, для більш коректної та продуктивної роботи мережі.

Мережа що була спроектована не мала надійного захисту від атак зловмисників. Отже, треба детально дослідити механізми безпеки, задля запобігання несанкціонованого доступу до мережі комунального підприємства.

При проектуванні безпроводової мережі був зроблений розподіл користувачів по класам виходячи з типу послуг якими вони будуть користуватися та інформаційна модель мережі. Мережа може надавати послуги безпроводового доступу до мережі інтернет, наприклад, такі, як користування соціальними мережами, забезпечення які надають можливість аудіо або відео спілкування, наприклад «Skype». Також не варто забувати про звичайне використання браузерів або електронної пошти, та послуги доступу до інформаційно-довідкового серверу.

2 РОЗРАХУНОК НАВАНТАЖЕННЯ ТА ПАРАМЕТРИ МЕРЕЖІ

2.1 Корегування розрахунків навантаження на мережу.

Одною з найважливіших частин у розробці та проектуванні мережі є розрахунок навантаження. Для того, щоб провести необхідні розрахунки необхідно притримуватись відповідної методики [7] та враховувати наступний перелік важливих параметрів:

— кількість абонентів

— вид трафіку

— параметри трафіку

У попередніх дослідженнях було розраховано навантаження на мережу, що проектується але при необхідності масштабувати її в амбулаторіях, а також через останніх обставин кількість відвідувачів збільшилась, тож усі параметри необхідно перерахувати. У попередніх розрахунках ми отримали результати зведені у таблиці 2.1:

Таблиця 2.1 — Пропускні здатності отримані при попередніх розрахунках

Найменування підприємства	Інтернет (web-серфінг), Мбіт/с	Інтернет (ел. пошта, соц. мережі) , Мбіт/с	Інтернет телефонія, skype, Мбіт/с	Відеоконференції, Мбіт/с	Доступ до серверу, Мбіт/с	Всього , Мбіт/с
Амбулаторія «ЦПМСД» № 1	38,4	1,066	0,768	2,048	19,2	61,482
Амбулаторія «ЦПМСД» № 2	6,4	0,177	0,23	0,682	3,2	10,689
Амбулаторія «ЦПМСД» № 3	12,8	0,355	0,48	1,365	6,4	21,4
Амбулаторія «ЦПМСД» № 4	6,4	0,177	0,23	0,682	3,2	10,689
Амбулаторія «ЦПМСД» № 5	2,56	0,071	0,115	0,273	1,28	4,299
Амбулаторія «ЦПМСД» № 6	6,4	0,177	0,23	0,682	3,2	10,689
Амбулаторія «ЦПМСД» № 10	3,84	0,106	0,192	0,478	1,92	6,536

Головною методикою у розрахунку трафіка виступають характеристики потоку даних котрі генеруються додатками у мережі [8]. Для кожного виду послуга трафік повинен розраховуватись окремо. Для розрахунку будемо використовувати наступну формулу:

$$\gamma_i^{(k)} = B_{ср}^{(k)} \cdot N_{аб_i}^{(k)} \cdot T_c^{(k)} \cdot f_{викл_i}^{(k)}, \quad (2.1)$$

де: k – номер мережної послуги;

i – номер вузла;

$\gamma_i^{(k)}$ – математичне очікування трафіка;

$B_{ср}^{(k)}$ – швидкість передачі даних (у бітах або пакетах у секунду);

$N_{аб_i}^{(k)}$ – кількість абонентів на *i-му* вузлі, які користуються *k-ою* послугою;

$T_c^{(k)}$ – середня тривалість сеансу зв'язку для *k-ої* послуги;

$f_{викл_i}^{(k)}$ – середня кількість викликів у годину найбільшого навантаження для користувачів *i-го* вузла, які використають *k-у* послугу.

Швидкість передачі даних розраховується наступною формулою:

$$B_{ср}^{(k)} = \frac{B_{max}^{(k)}}{P^{(k)}}, \quad (2.2)$$

де: $B_{ср}^{(k)}$ – максимальна пропускна здатність каналу зв'язку;

$P^{(k)}$ – пачечність одного абонента.

Далі потрібно розрахувати навантаження на мережу, а для цього необхідно визначити кількість абонентів на кожному вузлу мережі (таблиця 2.1). Проводити розрахунки будемо за методикою викладеною вище. Результати розрахунків викладені у таблиці 2.2.

Таблиця 2.2 – Розподіл користувачів за вузлами та послугами

Найменування підприємства	Тип послуги	Кількість користувачів
Амбулаторія «ЦПМСД» № 1	Інтернет (web-серфінг)	250
	Інтернет (ел. пошта, соц. мережі)	250
	Інтернет телефонія, skype	80
	Відеоконференції	60
	Доступ до серверу	250
Амбулаторія «ЦПМСД» № 2	Інтернет (web-серфінг)	50
	Інтернет (ел. пошта, соц. мережі)	50
	Інтернет телефонія, skype	35
	Відеоконференції	25
	Доступ до серверу	50
Амбулаторія «ЦПМСД» № 3	Інтернет (web-серфінг)	80
	Інтернет (ел. пошта, соц. мережі)	80
	Інтернет телефонія, skype	55
	Відеоконференції	45
	Доступ до серверу	80
Амбулаторія «ЦПМСД» № 4	Інтернет (web-серфінг)	45
	Інтернет (ел. пошта, соц. мережі)	45
	Інтернет телефонія, skype	25
	Відеоконференції	20
	Доступ до серверу	45
Амбулаторія «ЦПМСД» № 5	Інтернет (web-серфінг)	20
	Інтернет (ел. пошта, соц. мережі)	20
	Інтернет телефонія, skype	12
	Відеоконференції	8
	Доступ до серверу	20
Амбулаторія «ЦПМСД» № 6	Інтернет (web-серфінг)	40
	Інтернет (ел. пошта, соц. мережі)	40
	Інтернет телефонія, skype	20
	Відеоконференції	15
	Доступ до серверу	40
Амбулаторія «ЦПМСД» № 10	Інтернет (web-серфінг)	30
	Інтернет (ел. пошта, соц. мережі)	30
	Інтернет телефонія, skype	20
	Відеоконференції	15
	Доступ до серверу	30

Зробимо розрахунок навантаження для амбулаторій, та розглянемо проведення розрахунків на прикладі Амбулаторія «ЦПМСД» № 1. Для цього нам потрібно скористуватися формулами 2.1 та 2.2.

Проведемо приклад розрахунку для амбулаторії №1. Для розрахунку скористаємося формулами 1.1 та 1.2, вихідними даними будуть параметри послуг, що зведені в таблиці 1.3, та кількість абонентів зведених у таблиці 2.1:

Розрахунок навантаження для послуги:

— Інтернет (web-серфінг):

$$\gamma_1^{(k)} = B_{ср}^{(k)} \cdot N_{аб1}^{(k)} \cdot T_c^{(k)} \cdot f_{викл1}^{(k)} = \frac{2{,}048}{4} \cdot 250 \cdot 600 \cdot \frac{3}{3600} = 64\ Мбіт/с;$$

— Інтернет (електронна пошта, соціальні мережі):

$$\gamma_2^{(k)} = B_{ср}^{(k)} \cdot N_{аб2}^{(k)} \cdot T_c^{(k)} \cdot f_{викл2}^{(k)} = \frac{0{,}512}{2} \cdot 250 \cdot 10 \cdot \frac{10}{3600} = 1{,}78\ Мбіт/с;$$

— Інтернет телефонія, skype:

$$\gamma_2^{(k)} = B_{ср}^{(k)} \cdot N_{аб2}^{(k)} \cdot T_c^{(k)} \cdot f_{викл2}^{(k)} = \frac{0{,}128}{1} \cdot 80 \cdot 180 \cdot \frac{3}{3600} = 1{,}54\ Мбіт/с;$$

— Відеоконференції:

$$\gamma_2^{(k)} = B_{ср}^{(k)} \cdot N_{аб2}^{(k)} \cdot T_c^{(k)} \cdot f_{викл2}^{(k)} = \frac{1{,}024}{1} \cdot 60 \cdot 240 \cdot \frac{1}{3600} = 4{,}1\ Мбіт/с;$$

— Доступ до інформаційного серверу:

$$\gamma_2^{(k)} = B_{ср}^{(k)} \cdot N_{аб2}^{(k)} \cdot T_c^{(k)} \cdot f_{викл2}^{(k)} = \frac{1{,}024}{2} \cdot 250 \cdot 180 \cdot \frac{5}{3600} = 32\ Мбіт/с;$$

Підсумувавши потоки по кожному з типу послуг, загальна величина пропускної здатності каналу зв’язку, що мінімально необхідна для одного користувача становить $\gamma_{загальне} = 103{,}4\ Мбіт/с$, з яких 67,3 *Мбіт/с* приходиться на послугу Інтернет [9].

Згідно з розрахунків вище необхідно зробити теж саме для інших амбулаторій. Результати усіх підрахунків для КП «ЦПМСД» Покровської міської ради приведені у Таблиці 2.3

Таблиця 2.3 – Скореговані сумарні пропускні здатності

Найменування підприємства	Інтернет (web-серфінг), Мбіт/с	Інтернет (ел. пошта, соц. мережі) , Мбіт/с	Інтернет телефонія, skype, Мбіт/с	Відеоконференції, Мбіт/с	Доступ до серверу, Мбіт/с	Всього , Мбіт/с
Амбулаторія «ЦПМСД» № 1	64	1,78	1,54	4,1	32	103,4
Амбулаторія «ЦПМСД» № 2	12,8	0,36	0,67	1,71	6,4	21,9
Амбулаторія «ЦПМСД» № 3	20,48	0,57	1,06	3,07	10,24	35,4
Амбулаторія «ЦПМСД» № 4	11,52	0,32	0,48	1,37	5,76	19,5
Амбулаторія «ЦПМСД» № 5	5,12	0,14	0,23	0,55	2,56	8,6
Амбулаторія «ЦПМСД» № 6	10,24	0,28	0,38	1,02	5,12	17,1
Амбулаторія «ЦПМСД» № 10	7,68	0,21	0,38	1,02	7,68	17

Нижче наводжу результати розрахунків необхідної пропускної здатності на одного користувача в Таблиці 2.4

Таблиця 2.4 – Пропускні здатності на одного користувача

Найменування підприємства	Сумарні пропускні здатності	Кількість користувачі	Пропускні здатності на одного користувача
Амбулаторія «ЦПМСД» № 1	103,3	250	0,413
Амбулаторія «ЦПМСД» № 2	21,9	50	0,438
Амбулаторія «ЦПМСД» № 3	35,4	80	0,442
Амбулаторія «ЦПМСД» № 4	19, 5	45	0,433
Амбулаторія «ЦПМСД» № 5	8,6	20	0,43
Амбулаторія «ЦПМСД» № 6	17, 1	40	0,427
Амбулаторія «ЦПМСД» № 10	17	30	0,566

Отже, порівнюючи попередні розрахунки та розрахунки з урахування корегувань, можемо побачити, що навантаження на мережу зросло майже у два рази, що дуже значно позначиться при проектуванні мережі [10].

2.2 Корегування стандартів та технологій безпроводового доступу.

Під час попереднього проектування вже були розглянути стандарти та технології безпроводових мереж доступу. Мною був обраний стандарт 802.11ac (Wi-Fi 5), але останнього часу набирає популярності новий стандарт 802.11ax (Wi-Fi 6), який у порівнянні з попереднім поколінням має багато переваг [11].

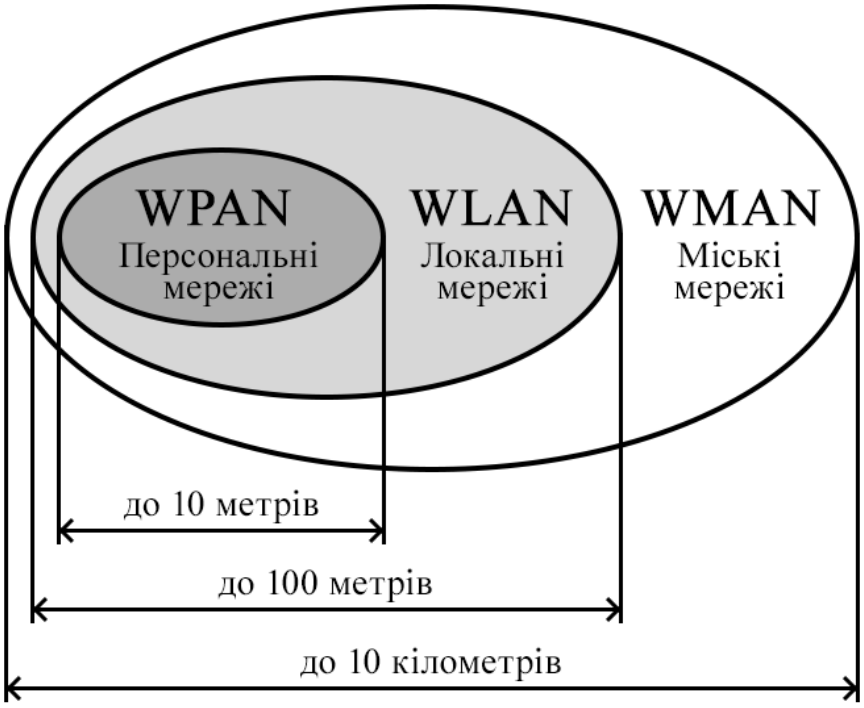


Рисунок 2.1 — Класифікація безпроводових мереж

Технологія Wi-Fi 6 — IEEE 802.11ax — новий стандарт безпроводових інтернет мереж, цей стандарт призначений для роботи у вже існуючим спектрі діапазонів 2,4 ГГц та 5 ГГц, але може мати додаткові смуги частот у діапазонах

від 1 до 7 ГГц у мірі їх появи. У додатку до використання технологій MIMO та MU-MIMO , у новому стандарті IEEE 802.11ax додається режим ортогонального частого мультиплексування для покращення спектральної ефективності, а також модуляція 1024-QAM для звеличення пропускної здатності. Хоча початкова швидкість передачі даних лише на 37% більш, ніж у попередньому стандарті IEEE 802.11ac. Очікується, що новий стандарт дозволить у чотири рази покращити середню пропускну здатність завдяки більш ефективного використання спектра та покращень у розгортанні [12].

2.2.1 Порівняння безпроводових технологій IEEE 802.ac та IEEE 802.11ax.

Зміни у 802.11ax має декілька головних змін у порівнянні з 802.11ac [13]:

OFDMA — у стандарті 802.11ac ця особливість недоступна, на відміну від 802.11ax, де ця особливість надає централізовано контрольований доступ до частини з динамічним значенням.

Багатокористувачевий MIMO (MU-MIMO) — у стандарті 802.11ac ця особливість доступна лише у направленні вниз, а у стандарті 802.11ax доступно у двох направленнях — вниз та вгору.

Випадковий доступ на основі тригеру — у попередньому стандарті недоступний, а у новому ця особливість дозволяє виконувати передачі UL OFDMA станціями, яким RU не назначені напряму.

Повторне використання просторової частоти — у попередньому стандарті недоступний. У новому ця особливість дозволяє відлічати передачі у своїй мережі від передач в іншій. А також, поріг адаптивної потужності та чутливості дозволяє динамічно регулювати потужність передачі та поріг визначення сигналу для збільшення просторового повторного використання.

Вектор розподілу мережі — у попередньому стандарті ця особливість мала одинарний вектор, у новому стандарті цей вектор подвійний.

Цільовий час пробудження — у попередньому стандарті недоступний, а у новому цільовий час пробудження понижує енергоспоживання та середній доступ до мережі.

Фрагментація — у минулому стандарті вона статична, а у новому динамічна, що допомагає понизити накладні витрати.

Тривалість захисного інтервалу — у стандарті 802.12ac він складає 0,4 мкс або 0,8 мкс, а у стандарті 802.11ax тривалість складає 3,2 мкс, 6,4 мкс, або 12,8 мкс, що дозволяє значно збільшити захист від поширення затримки сигналу.

Тривалість символу — у попередньому стандарті вінд складає 3,2 мкс, а у новому 3,2 мкс, 6,4 мкс або 12,8 мкс, що дозволяє підвищити ефективність.

Отже, серед головних відмінностей можна виділити наступні переваги наведені у таблиці 2.5.

Таблиця 2.5 — головні відмінності стандартів Wi-Fi 5 та Wi-Fi 6

Відмінність	802.11ac	802.11ax
Швидкість мережі	до 433 Мбіт/с	до 1,2 Гбіт/с
Пропускна здатність	до 32 пристроїв	до 128 пристроїв
Затримка сигналу	30 мс	10 мс
Енергоефективність	х/с	Х*70%/с

Як ми можемо бачити, новий стандарт IEEE 802.11ax пропонує дуже великі покращення у пропускній здатності — до 128 пристроїв на одну точку доступу, що є дуже важливим для проектування нашої мережі. А також

технологія Wi-Fi 6 має значно меншу затримку та на 30% більшу енергоефективність.

Під час проектування WLAN та WPAN мереж використовують ці технології. Різниця між цими технологіями у робочих частотах та характеристиках інтерфейсу визначена у таблиці 2.6

Таблиця 2.6 — Класифікація безпроводових технологій

Безпроводові технології					
WLAN		WPAN		BWA	
2,4 ГГц	**5 ГГц**	**2,4 ГГц**	**5 ГГц**	**2-10 ГГц**	**10-66 ГГц**
802.11	802.11a	802.15.1	HiperPAN	802.16.3	802.16.1
802.11b	802.11n	802.15.3		MMDS	LMDS
802.11g	802.11ax	802.15.4		WDSL	
802.11n	HiperLan1/2				
	HiSWAN				

Після проведення аналітики над класифікаціями, що приведені у таблиці віще, можна зробити висновки, що проектуєма мережа відноситься до класу WLAN. Головною задачею безпроводових локальних мереж організовувати доступ до інтернет-мережі в середині будівель, наприклад, організація суспільних точок доступу у місцях великого скупчення людей, наприклад, як раз у амбулаторіях. Для розгортання мережі що проектується буде використана технологія IEEE 802.11, яка підходить для користування через смартфони або ноутбуки.

2.3 Синтез структурної схеми.

Синтез структурної схеми необхідний для того, щоб наглядно показати як мережа повинна виглядати в цілому. До мережі, яка проектується входять наступні пристрої: комутатори розподілу працюючі на 3 рівні моделі OSI та точки доступу, які до них приєднуються. На кожному з комутаторів необхідний хоча б один порт, який підтримує технологію 1000BASE-TX.

Точки доступу які будуть обрані мають працювати у режимі 802.11ax на діапазоні частот 2,4 ГГц та 5 ГГц. Безпроводовий сегмент мережі повинен надавати пропускну здатність 72 Мбіт/с при радіусі зони покриття 15 метрів.

Провівши перерахунки навантаження на мережу було отримано максимальне навантаження на мережу — 104 Мбіт/с. У мережі, що проектується буде використана топологія зв’язку зірка.

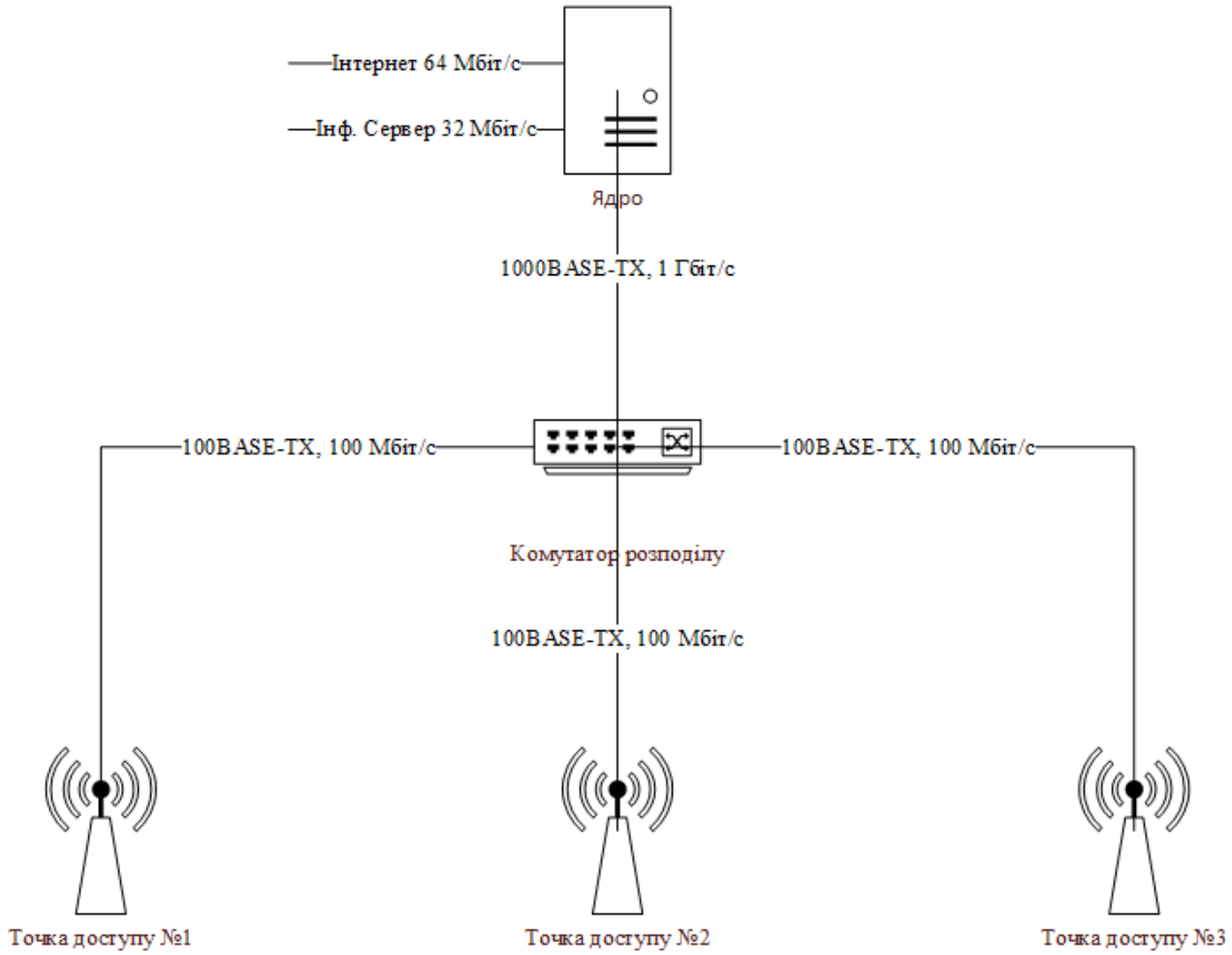


Рисунок 2.2 – Структурна схема мережі

2.4 Вибір кінцевого обладнання.

Робити вибір кінцевого обладнання, а саме точок доступу будемо на основі тих вимог, які потребує мережу, котру будемо проектувати. Згідно з характеристик мережи нас цікавлять наступні вимогу до точок доступу:

— підтримують 1000BASE-TX технологію;
— мають RJ-45 інтерфейс;
— підтримка нового стандарту 802.11ax;
— пропускна здатність від 100 Мбіт/с;
— підтримка WEP, WPA, PoE протоколів.

Провівши аналітику серед існуючих на українському ринку пристроїв серед тих, що відповідають до вище складених вимог мій вибір пав на точку доступу від компанії Huawei — Wi-Fi AX3. Ці точки доступу мають технологію Dynamic Narrow Bandwidth на базі Chipset Synergy завдяки якої вони здатні передавати сигнал, посилений на 6 дБ, у вузькосмуговому режимі 2 МГц. Безпроводовий сигнал легко може проходити скрізь стіни та підлогу, отже пристрої можуть горно приймати сигнал на великій відстані навіть на іншому поверсі. Завдяки 1024-QAM схемі модуляції та смузі пропускання на 160 МГц швидкість сигналу може сягати до 3 Гбіт/с: до 600 Мбіт/с при частоті 2,4 ГГц та до 2,4 Гбіт/с при частоті 5 ГГц. Роутер має центральний процесор Gigahome на чотири ядра, що виводить на новий рівень швидкість сигналу, відтепер буферизація та затримки значно нижче. Точка доступу має можливість підключення великої кількості пристроїв без значної шкоди для продуктивності. З технологією OFDMA точка доступу передає дані кільком пристроям одночасно, а у подвійному діапазоні до маршрутизатора можна приєднати до 128 пристроїв. З Huawei WiFi AX3 можна створити мережу з

кількох точок доступу, після об’єднання кілька роутерів, вони створюють одну мережу зі спільною назвою, а абоненти будуть приєднуватись до оптимальної точки доступу в залежності від їх розташування. Точка доступу має вбудовану систему безпеки, яка гарантує захист даних на програмному та апаратному рівні. Роутер отримав сертифікат CC EAL5, що означає безпечну роботу в комерційному середовищі та гарантує високий рівень захисту пристроїв.

2.4.1. Корегування кількості точок доступу.

У попередніх дослідженнях було проведено розрахунок кількості точок доступу для підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради. Розрахунки проводились за наступною методикою: маючи характеристики підприємств, була підрахована необхідна кількість кінцевих пристроїв, що зведено у таблиці 2.7

Таблиця 2.7 — Характеристика будівель та кількість точок доступу

	Абоненти	V, Мбіт/с	Qs	W, m	L, m	w/l, m	r	c	Qv
Амбулаторія №1	250	0,425	2	13,7	48,8	17,115	1	3	12
Амбулаторія №2	50	0,425	1	12,6	44,5	17,115	1	3	3
Амбулаторія №3	80	0,425	2	13,25	110,2	17,115	1	6	6
Амбулаторія №4	45	0,425	1	12,9	31,8	17,115	1	2	2
Амбулаторія №5	20	0,425	1	11,8	13,6	17,115	1	1	1
Амбулаторія №6	40	0,425	1	13,1	43,6	17,115	1	3	3
Амбулаторія №10	30	0,425	1	13,4	23	17,115	1	2	2

Зробивши підрахунки було обрано кількість точок доступу виходячи з геометричних параметрів будівель. Але, зараз потрібно скорегувати кількість кінцевих пристроїв, до кожної амбулаторії необхідно додати по одному пристрою біля входу до будівлі, тому що під час карантину відвідувачі амбулаторій примушені чекати свої черги на вулиці, а при проектуванні зона

покриття поза межами будівель не була врахована. Отже, проведемо корегування по наступній формулі:

$$Q_{V2} = Q_V + 1 \tag{2.3}$$

Таблиця 2.8 — Скорегована кількість кінцевих пристроїв

	Кількість точок доступу
Амбулаторія №1	13
Амбулаторія №2	4
Амбулаторія №3	7
Амбулаторія №4	3
Амбулаторія №5	2
Амбулаторія №6	4
Амбулаторія №10	3

Провівши перерахунок кількості точок доступу для побудови мережі безпроводового доступу комунального підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради на базі стандарту технології IEEE 802.11ax необхідно 36 точок доступу, з пропускною здатністю на кожному пристрої від 20 Мбіт/с.

2.5 Моделювання зони покриття безпроводової мережі.

Після зроблених розрахунків було отримано необхідну кількість точок доступу для побудови мережі, котра дорівнює в загальному по площі 36 одиницям точок доступу для усіх підприємств. Отже, тепер необхідно визначити розташування пристроїв. Розташування точок доступу було виконано за площею будівель, тому що кількість користувачів є не занадто щільною, та проблем з недостатньою пропускною здатністю не повинно

виникати, та якщо посилатися на пропускну здатність, то не вдасться покрити усю активну площину будівель безпроводовою інтернет мережею. Схема розташування кінцевих пристроїв в амбулаторіях наведена в Додатку А.

Висновки до розділу 2

Для проектування мережі з урахуванням сучасних проблем були перераховані та скореговані вимоги до мережі, завдяки чому ми з’ясували, що мережа зазнала помітних змін — кількість прогнозованих абонентів збільшилась, а отже навантаження на мереж теж зросло.

Також були переглянуті стандарти та технології які потребує мережа, що проектується. Був обраний більш відповідний для цілей стандарт. Було вирішено обрати стандарт IEEE 802.11ax, та через це зміни торкнулися і кінцевого обладнання — замість TP-Link Deco M5 були обрані інші точки доступу — Huawei WiFi AX3.

Для наглядного прикладу мережі яка проектується, то враховуючи вимоги до мережі було розроблено синтез структурної схеми. Після цього була перерахована кількість точок доступу для кожного підприємства, та з урахуванням розташування приладів за площею будівель був отриманий результат у 36 точок доступу на кожне підприємство та перебудовані схеми розміщень кінцевих обладнань. У завершенні підрахунку параметрів було змоделювано зону покриття безпроводової мережі — обрано місця розташування точок доступу за розрахованою кількістю та розміщено їх за площею будівель.

3 ЧАСТОТНЕ РАДІОПЛАНУВАННЯ МЕРЕЖІ

3.1 Загальні положення при частотному радіопланування мережі.

При проектуванні безпроводової мережі інтернет доступу необхідно дотримуватись збірки правил, яких слід дотримуватися. Серед великої збірки правил можна виділити самі головні:

— Вибір типу послуг;
— Щільність користувачів;
— Вимоги до пропускної здатності;
— Особливості пристроїв абонентів;
— Вимоги до безпеки мережі.

Приведені вище вимоги можуть бути виконані за допомогою використання наступних фізичних величин:

— Частотний діапазон;
— Канали обраного діапазону;
— Потужність передавача;
— Коефіцієнт потужності передавача;
— Дозволені швидкості передачі даних.

У частотному діапазоні 5 ГГц кількість каналів які не перетинаються значно більш ті вища пропускна здатність, але не зовсім кожен пристрій може підтримувати цей діапазон. Чого не можна сказати про частотний діапазон 2,4 ГГц, який підтримує кожен пристрій. У цьому діапазоні лише три канали які не перетинаються, це 1, 6 та 11, що необхідно ураховувати при частотному плануванні. Якщо розмістити дві точки доступу, які працюють на одному частотному діапазоні поруч, це може призвести до високого значення сигнал-шум. Якщо ми маємо велику площину, яку слід покрити мережею

безпроводового доступу, то можна розмістити до трьох Wi-Fi роутерів з метою підвищення пропускної здатності, але вони повинні працювати на різних канал та не заважати один-одному. Необхідно взяти до уваги, що корисна відстань зони покриття у діапазоні 2,4 ГГц значно вище, ніж у діапазоні 5 ГГц [14].

Для інтернет мережі необхідно визначити мінімальну швидкість передачі даних, наприклад, площу будівлі необхідно покрити безпроводовою мережею з 3 точок доступу, які будуть мати пропускну здатність 10 Мбіт/с, але якщо нам необхідно мати мінімальну пропускну здатність в 20 Мбіт/с, то слід розтушувати 6 точок доступу.

Якщо мережа проектується для використання голосової мережі необхідно враховувати те, що зона покриття між сусідніми точками доступу повинна перекриватися не менш, ніж на 10-20%, щоб забезпечити неперервний зв’язок під час спілкування.

При проектуванні мережі застосовується уважний підхід, адже за основу планування повинно враховуватися оптимальне розташування точок доступу, а не зона радіопокриття. Для збільшення зони покриття мережі не обов’язково збільшувати потужність передавача точки доступу, або пристрою клієнта, для цього застосовують антени. Отже, якщо необхідно покрити велику площу безпроводової мережі, то можна скористуватися зовнішніми антенами з великим коефіцієнтом посилення. Антени бувають як спрямованими — для довгих будівель, так і всеспрямованими — для великих будівель.

Також, при проектуванні мережі слід враховувати, що якщо нам потрібно одночасно підключення до мережи багатьох користувачів, то слід розташовувати точки доступу більш щільно, та зменшувати потужність передавача.

3.2 Дослідження програмного забезпечення для виміру показників.

Для виміру показників у середі, де буде спроектована безпроводова мережа було вирішено використовувати програмне забезпечення Wi-Fi Analyzer. В даний час практично скрізь можна знайти певну кількість загальнодоступних мереж Wi-Fi, але далеко не всі вони можуть надавати необхідну якість з'єднання і достатню пропускну здатність. Найчастіше рівень сигналу ніяк не пов'язаний з тим, на якій відстані від роутера ви перебуваєте, канал сам може мати обмеження по швидкості або ж мати сильну завантаженість. Wi-Fi Analyzer — це програма, за допомогою якої можна отримати всю необхідну і повну інформацію про доступні Wi-Fi каналі у середі та визначити найбільш відповідний і вільний для використання канал. Програма має наступні важливі функції:

— аналіз розподілу каналів;
— визначення якості каналу;
— аналіз інтерференції;
— надання звітів.

Принцип роботи додатків даного типу схожий, але різниця полягає в зручності використання, наявності додаткових функцій або ж в інтерфейсі. Результат в будь-якому випадку буде представлений у вигляді таблиці. Програми та додатки для аналізу мережі Інтернет дозволяють не тільки знайти найшвидший і зручний спосіб підключитися, але й виявити причину перебоїв в роботі або навіть злому. Завдяки таким програмам можна виявити найбільш вдале взаємне розташування пристроїв, оцінити вплив інших частот і, як результат, зробити з'єднання максимально стійким і швидким [15].

Користувач дуже швидко отримує доступ до всієї необхідної інформації. Досить провести перевірку і одразу буде доступно два вікна — у одному з них

можна вибрати найбільш підходящу для з'єднання мережу, а в іншому можна оцінити роботу кожного каналу зокрема. Вся інформація надається у вигляді таблиці, а різні кольори каналів допомагають не заплутатися. Додаткові переваги утиліти:

— визначає навіть найслабший сигнал у мережі;

— має датчики для визначення сили сигналу;

— безкоштовне завантаження додатку;

— вбирає нелегальні мережі і пристрої;

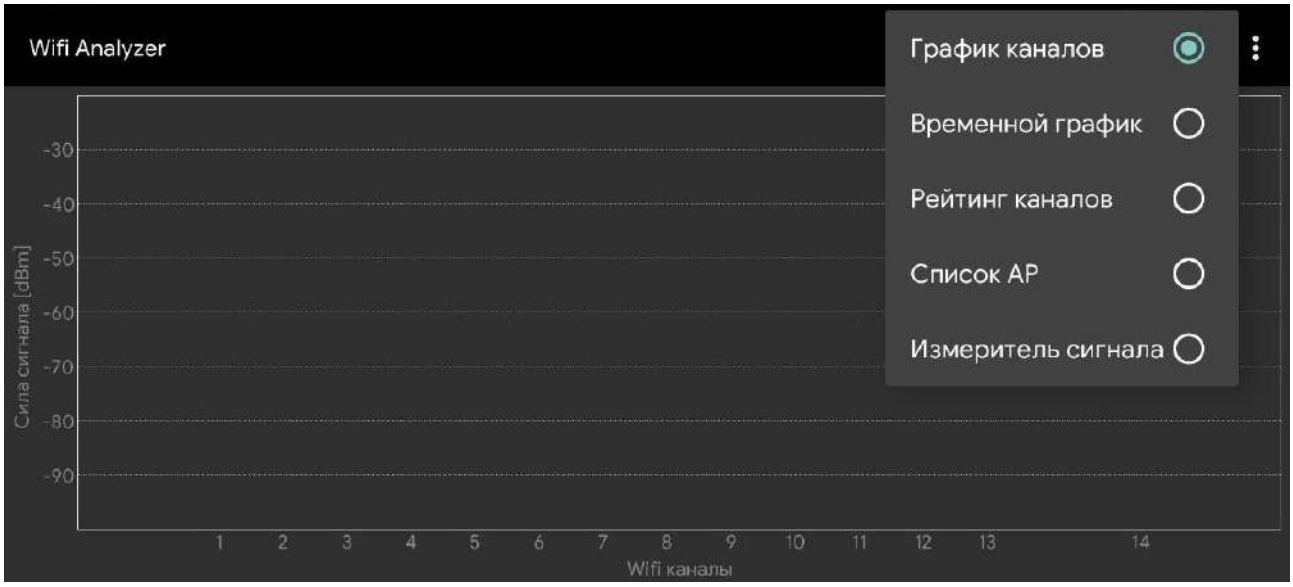


Рисунок 3.1 — Робоче середовище програми

Програма для смартфонів дуже проста у використанні. Досить запустити програму, далі почнеться автоматичне сканування всіх доступних підключень. Результат буде представлений у вигляді графіка. Версія для ПК виглядає приблизно так само. Сила сигналу буде відображатися у вигляді параболи, досить вибрати ту, яка вище. Завдяки графіками можна визначити, які мережі перетинаються, а які перериваються в конкретному місці розташування. Рейтинг каналів дозволяє за кількістю зірок визначити найменш схильне до

перешкод з'єднання. Також в списках AP можна знайти зведену інформацію про канал: режим безпеки, рівень сигналу та тип шифрування. Вимірювач сигналу допоможе визначити місцезнаходження джерела мережі, при наближенні до нього програма почне видавати все більш явні звукові сигнали. Кнопка «Tools» відображає всі пристрої в конкретної локальної мережі.

Найбільш корисні налаштування це:

— Автоматичне сканування;

— Завдання назви для доменів;

— Зміна інтервалів сканування;

— Автоматичне підключення до Wi-Fi;

— Тимчасове блокування реклами.

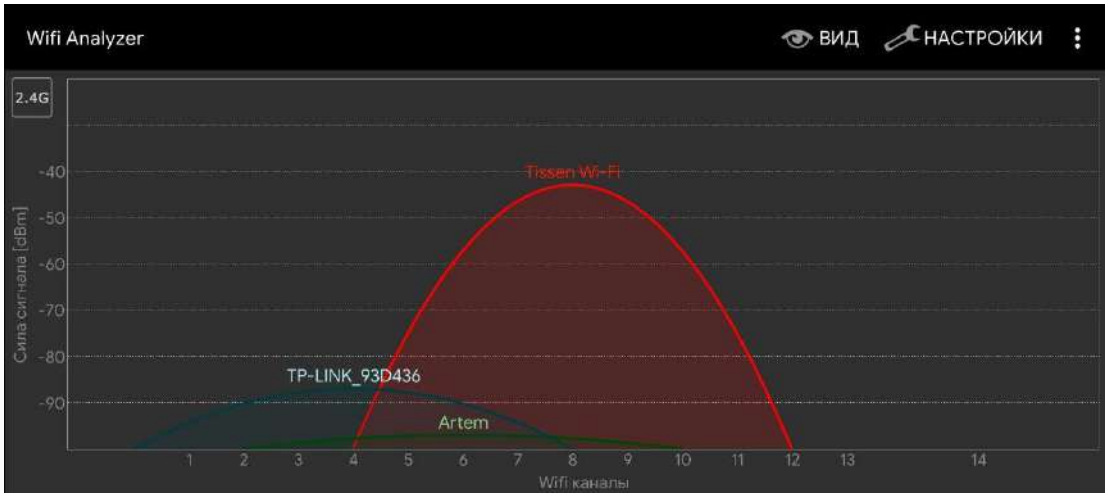


Рисунок 3.2 — Середовище сканування каналів та рівню сигналу

3.3 Аналіз середи у місці проектування безпроводової мережі.

Для проектування мережі необхідно проаналізувати середу, де буде розгорнуто безпроводову мережу. Завдяки мобільному додатку Wi-Fi Analyzer

було проведено спостереження над завантаженістю каналів задля того, щоб спроектована мережа надавала максимальну продуктивність [16].

Було проведено сканування мережі на трьох об’єктах для проектування мережі. На першому об’єкті Амбулаторії №1 за адресою вулиця Маршала Москаленко, будинок 161. Було виявлено понад 20 точок доступу, більшість з яких працюються у каналах від 2 до 11. Графіки показують використання SSID частоти та рівень сигналу передавача. Будівля є дуже довгою, тому показники було просканово у трьох місцях.

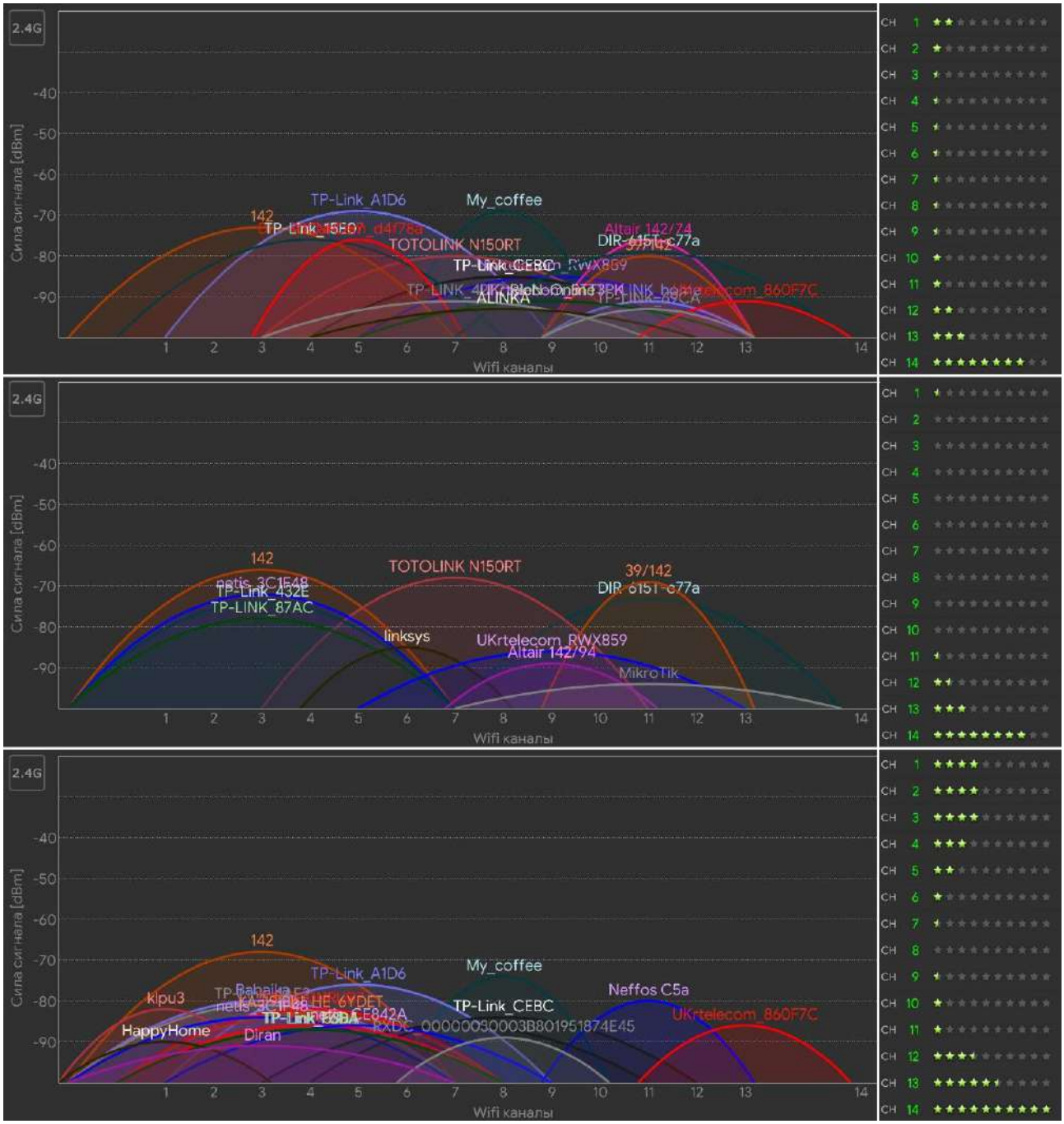


Рисунок 3.3 — Результати спостережень у Амбулаторії №1

Наступним об’єктом для аналізу середи безпроводової мережі була Амбулаторія №3 за адресою мікрорайон «Шахтарський», будинок 26-в/г. Так як амбулаторія знаходиться у жилому будинку, то кількість точок доступу доволі велика, іх було виявлено майже 25 пристроїв. Як бачимо, найбільш завантажені канали від 2 до 10. Об’єкт було просканово у двох місцях.

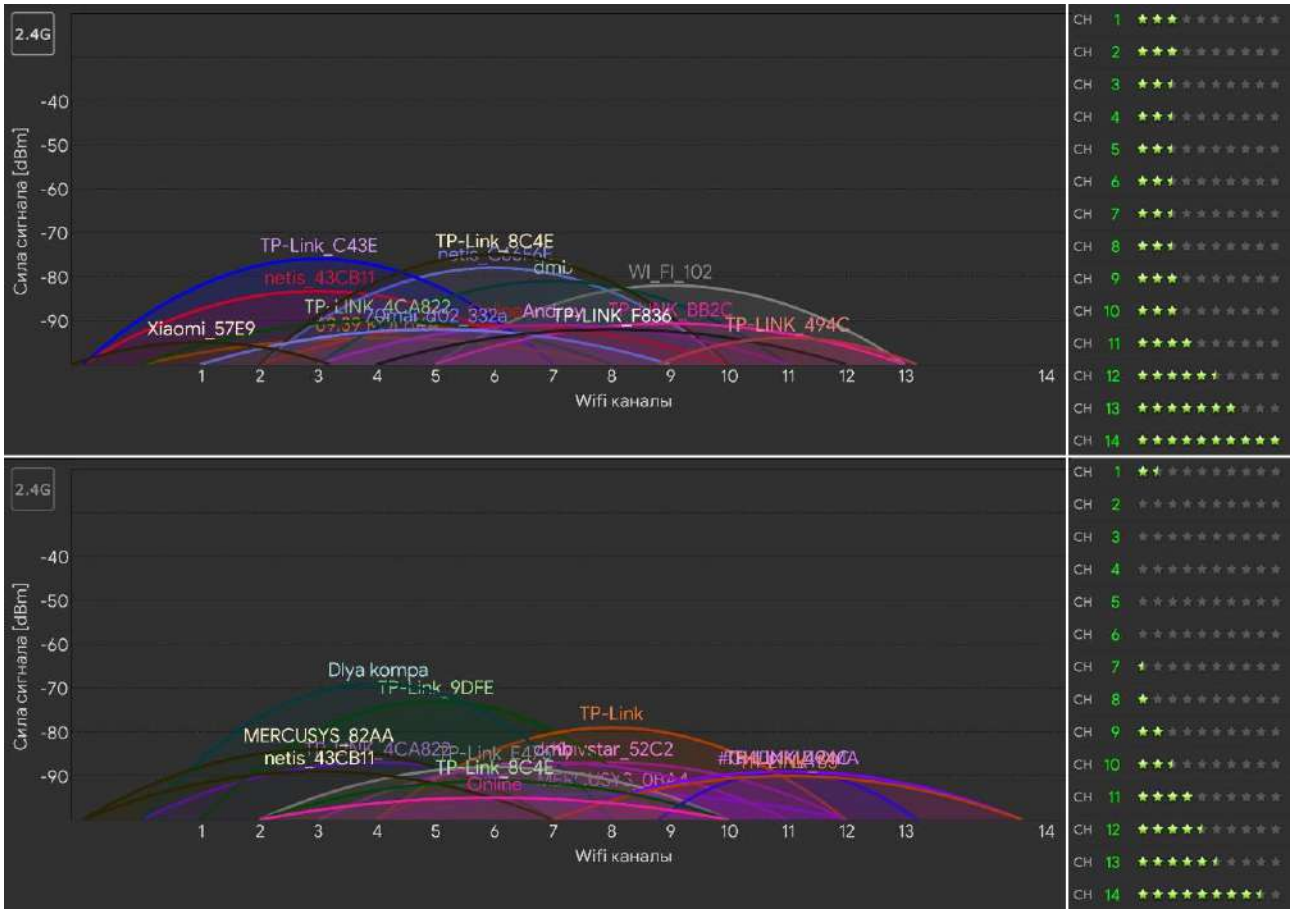


Рисунок 3.4 — Результати спостережень у Амбулаторії №3

Останнім об’єктом спостережень є Амбулаторія №10 за адресою вулиця Захисників України, будинок 33. Будівля розташована майже на окраїні міста, та на невеликій відстані від житлових будівель, тому кількість роутерів поблизу дорівнює усього 6 точок доступу, які найбільш навантажують канали у діапазоні від 2 до 11.

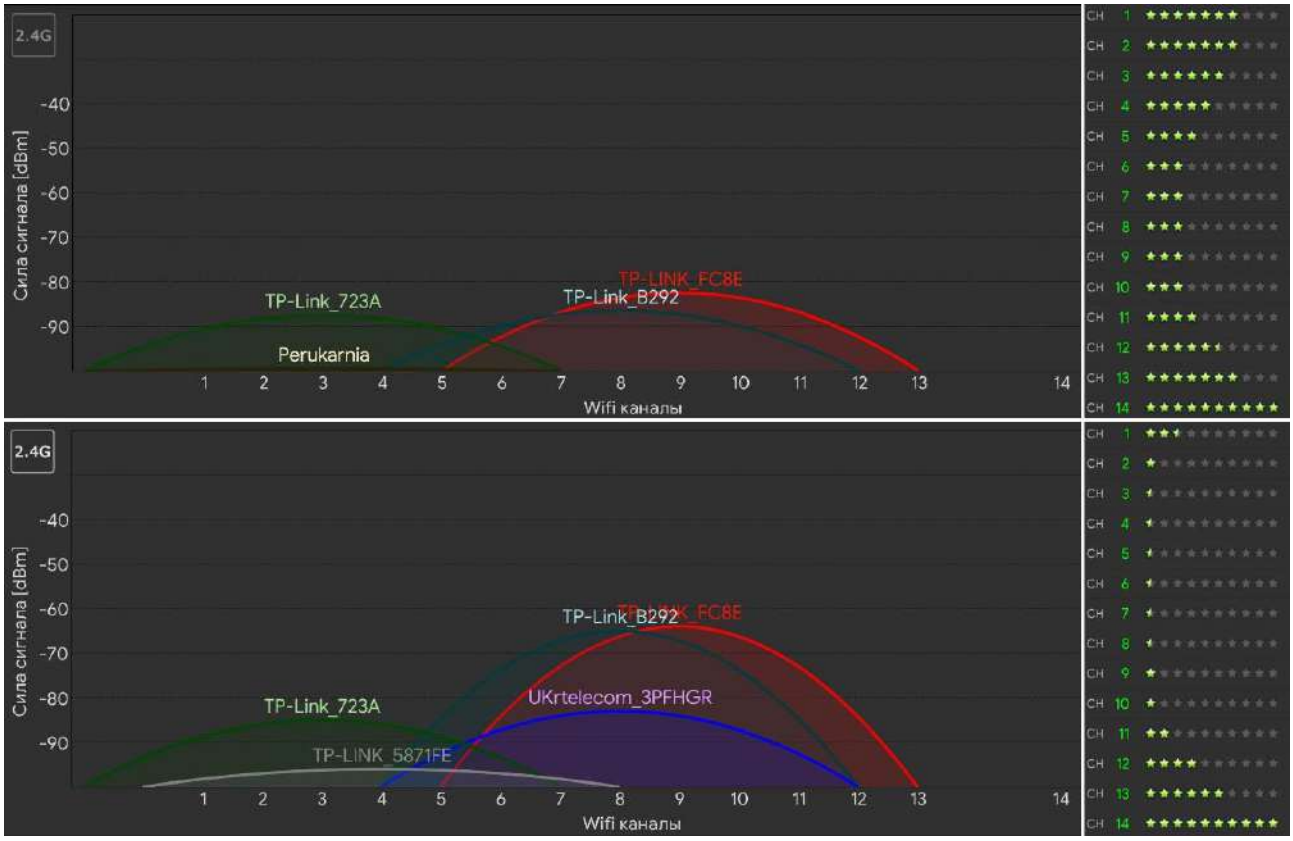


Рисунок 3.5 — Результати спостережень у Амбулаторії №10

Як результат спостережень можна зробити висновки, що деякі мережі мають досить навантажену середу та потрібно обирати найменш зайнять канали для роботи мережі.

3.4 Моделювання радіопокриття.

Щоб зробити моделювання безпроводової мережі буде використана спеціальна для цього програма Wi-Fi Planner, яка робить візуалізацію покриття безпроводової мережі. При застосуванні точок доступу Huawei WiFi AX3 застосовується функція автоматичного налаштування частоти.

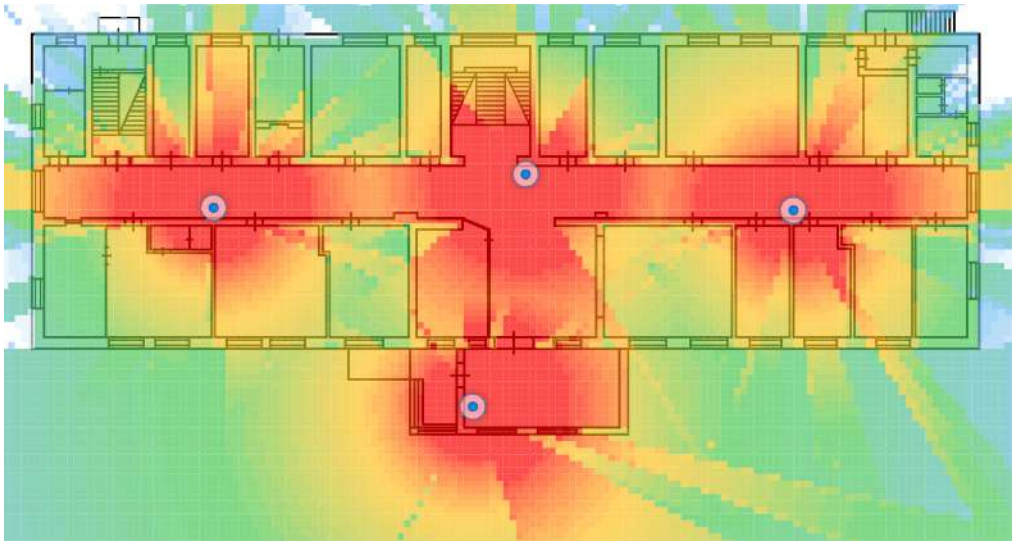


Рисунок 3.5 — Модель радіопокриття безпроводової мережи у Амбулаторії №1 (перший поверх)

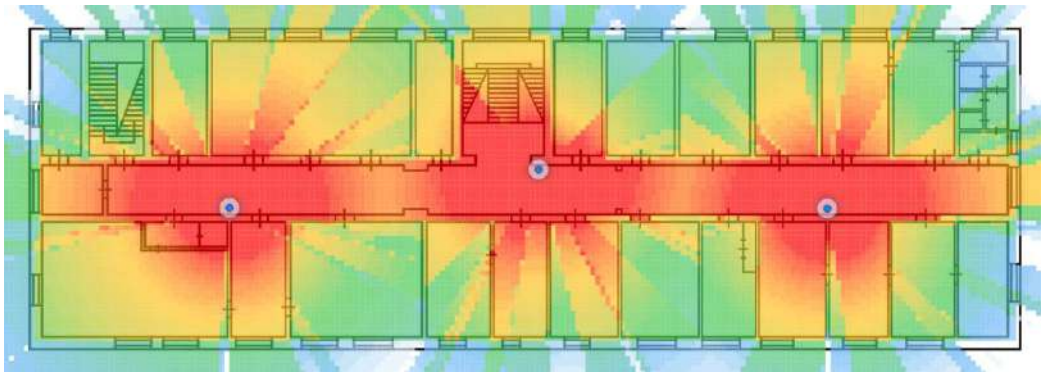


Рисунок 3.6 — Модель радіопокриття безпроводової мережи у Амбулаторії №1 (другий поверх)

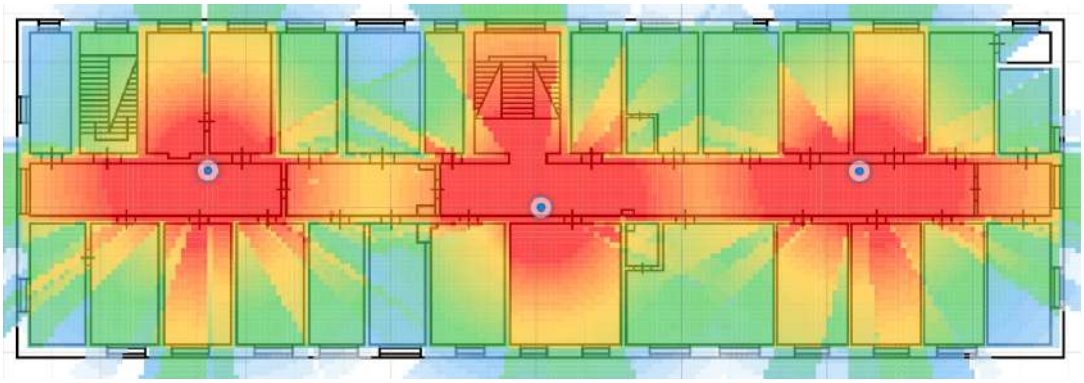


Рисунок 3.7 — Модель радіопокриття безпроводової мережи у Амбулаторії №1 (третій поверх)

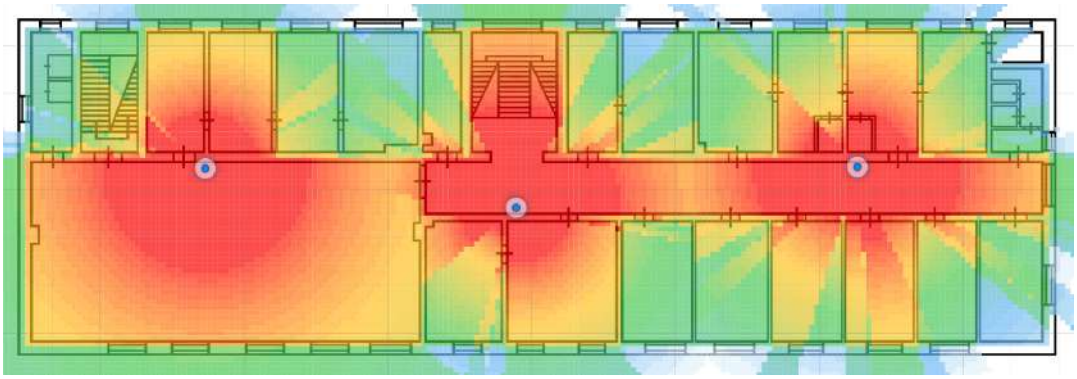


Рисунок 3.8 — Модель радіопокриття безпроводової мережі у Амбулаторії №1 (четвертий поверх)

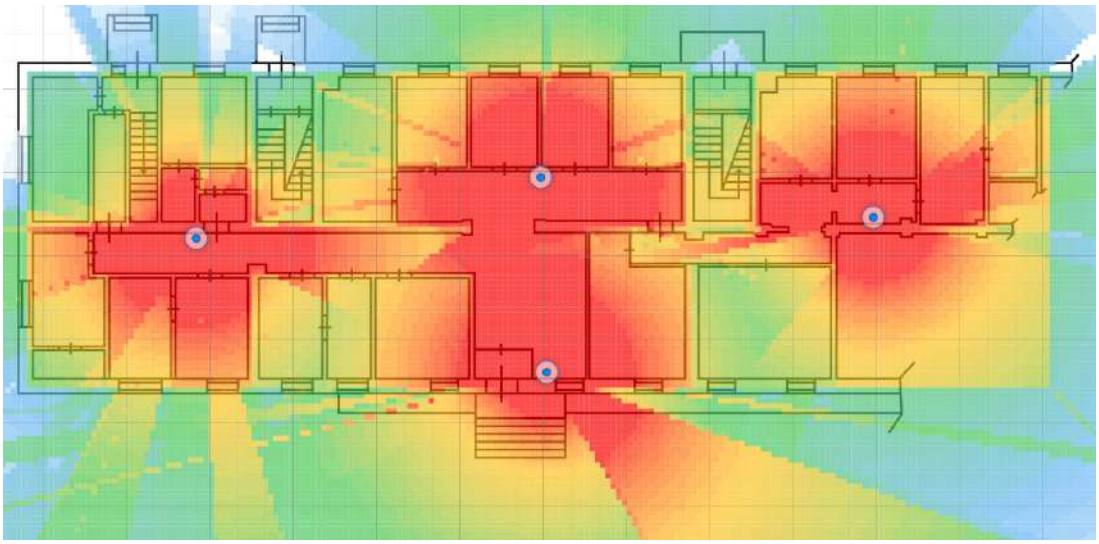


Рисунок 3.9 — Модель радіопокриття безпроводової мережі у Амбулаторії №2

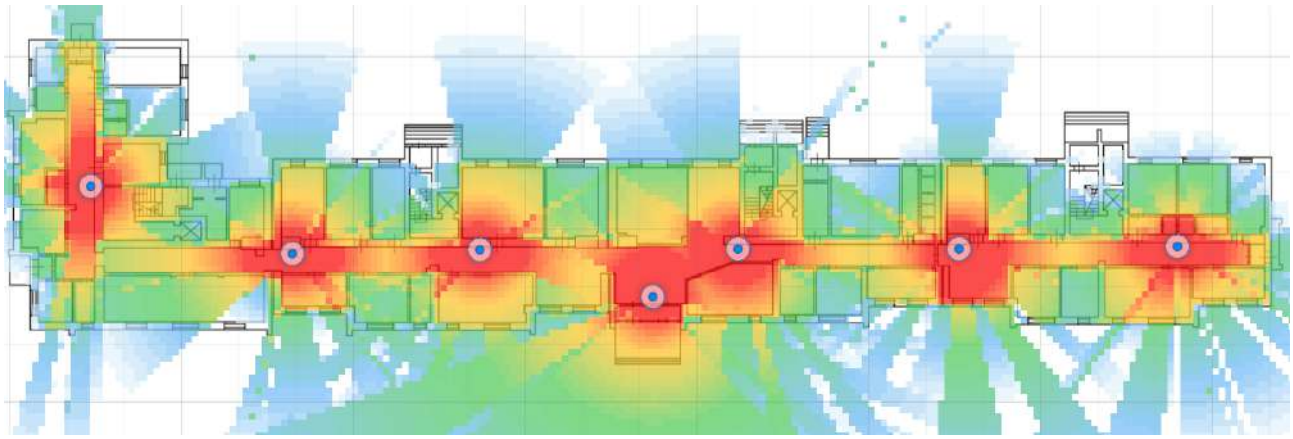


Рисунок 3.10 — Модель радіопокриття безпроводової мережі у Амбулаторії №3

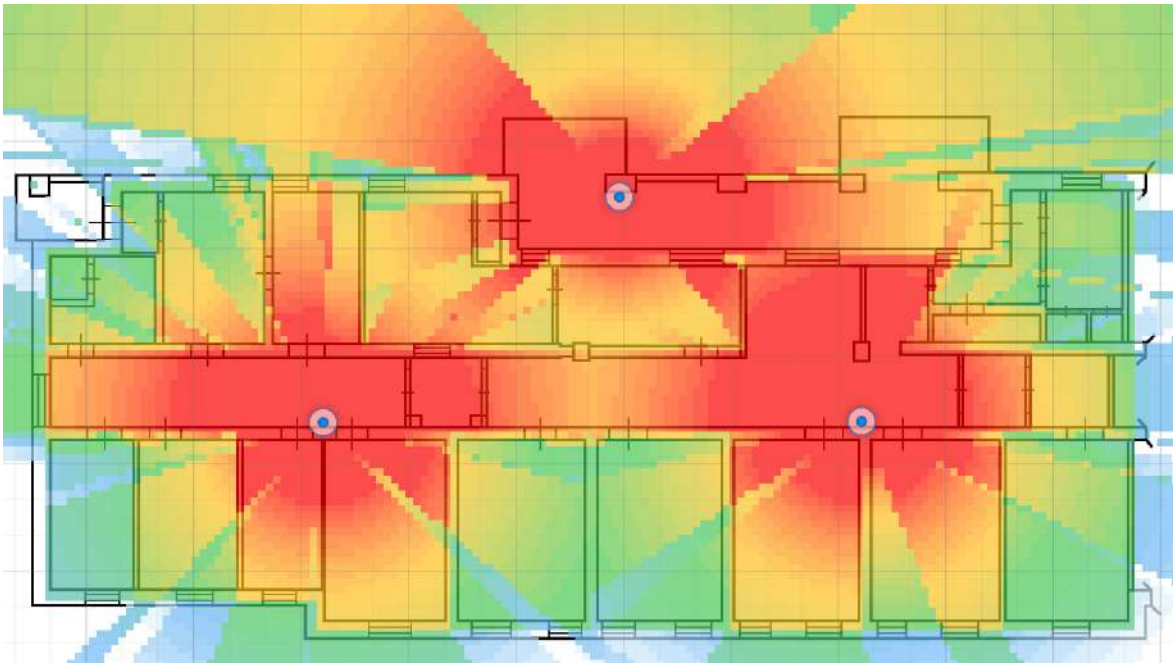


Рисунок 3.10 — Модель радіопокриття безпроводової мережі у Амбулаторії №4

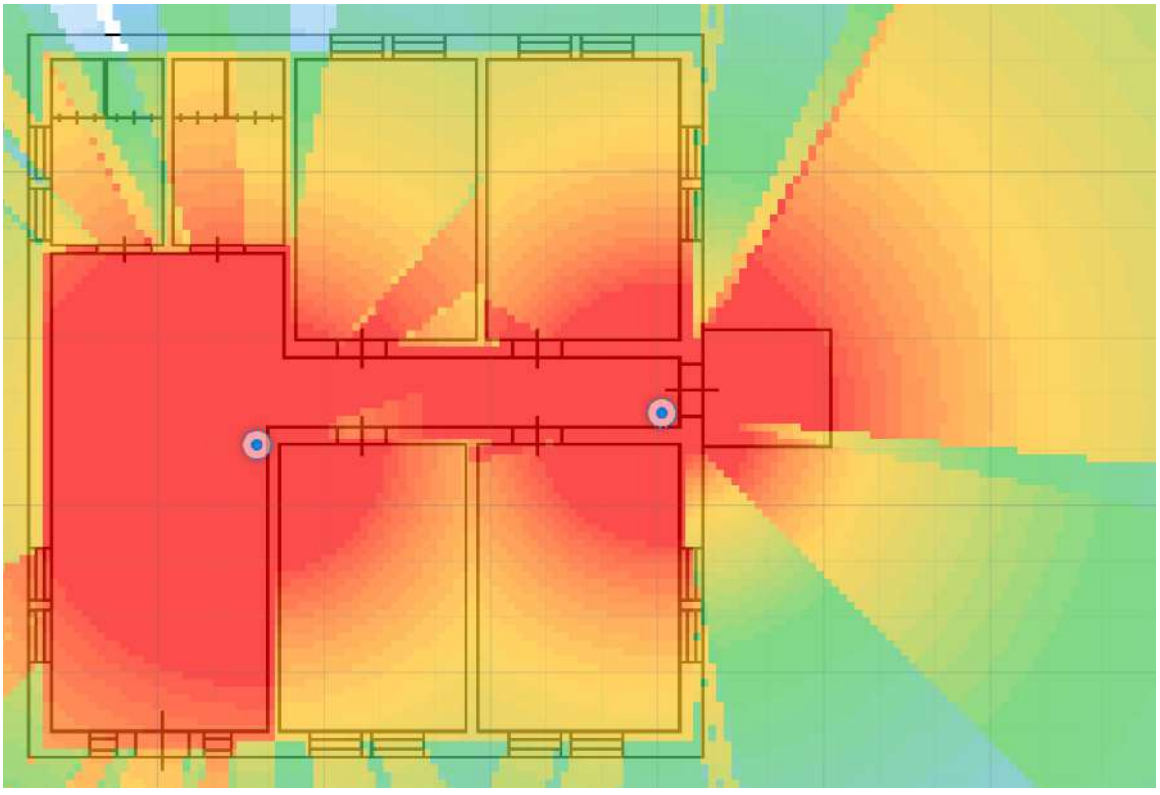


Рисунок 3.11 — Модель радіопокриття безпроводової мережі у Амбулаторії №5

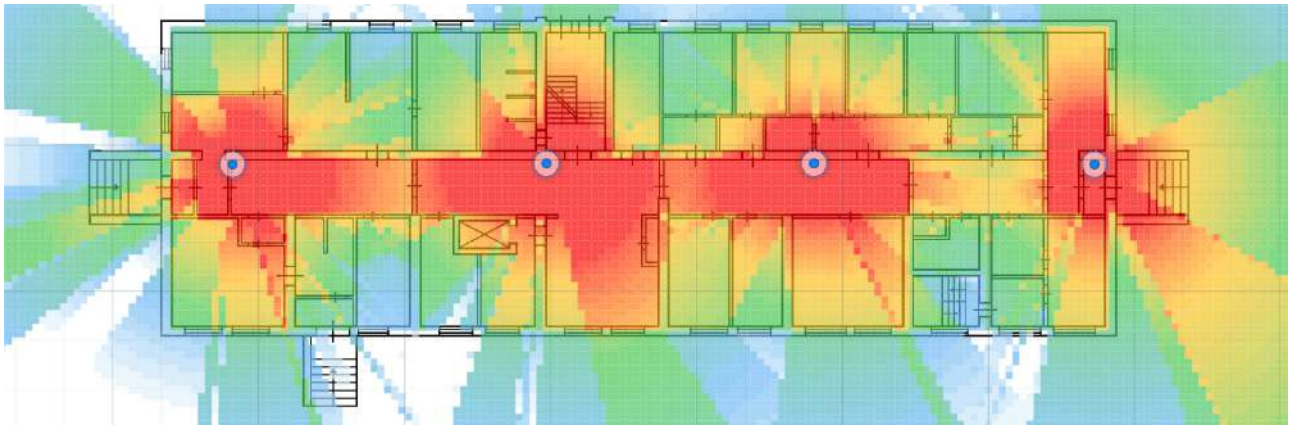


Рисунок 3.12 — Модель радіопокриття безпроводової мережі у Амбулаторії №6

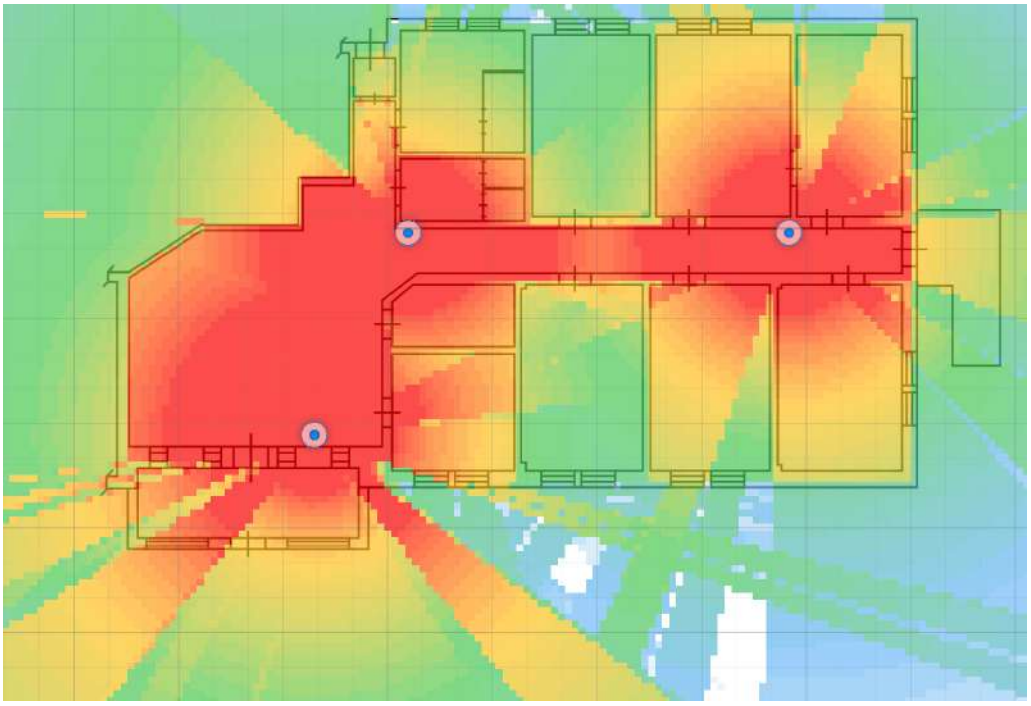


Рисунок 3.13 — Модель радіопокриття безпроводової мережі у Амбулаторії №10

Отже, зробивши моделювання радіопокриття, можна зробити висновки, що кількісті обраних точок доступу цілком вистачає для покриття об’єктів, де проектується безпроводова мережа. Майже усі будівлі мають 100% покриття площини, лише за рідким винятком дальні кути мають слабкий сигнал.

Висновки до розділу 3

У третьому розділі було розглянуто, чому важливо розробити радіомоделювання мережі і для чого це потрібно зробити. Окрім цього, було обрано програмне забезпечення Wi-Fi Analyzer та розглянуто його головні функції та переваги.

Використовуючи додаток Wi-Fi Analyzer було проаналізовано середовище трьох будівель де проектується безпроводова мережа, визначено завантаження каналів та кількість пристроїв у мережі.

Після аналізу середовища було зроблено радіомоделювання покриття мережі за допомогою додатка Wi-Fi Planner PRO від «D-Link» та за результатом моделювання зроблено висновки, що кількість та розташування точок доступу є оптимальним.

4 ДОСЛІДЖЕННЯ МЕХАНИЗМІВ БЕЗПЕКИ

4.1 Загальні положення безпеки безпроводових мереж.

Безпроводові локальні мережі забезпечують швидкий і простий доступ до інтернет-мережі та надає змогу пристроям дуже легко обмінюватися інформацією. Достатньо легко розгортаються та згортаються, але мають досить високу вразливість. Питання безпеки Wi-Fi стоїть сьогодні дуже гостро. Механізми аутентифікації і шифрування, які застосовуються в них в даний час, вкрай недосконалі. Саме тому користувачам доводиться вдаватися до інших інструментів. Паролі, фільтри та інші настройки безпеки бездротових з'єднань служать для певних цілей. Мережева безпека безпроводових мереж — найважливіше питання, якому слід приділити увагу при їх організації.

Одне з найголовніших питань, які необхідно вирішити при проектуванні безпроводової мережі — це захист. Майже кожного року з'являються нові технології, які дозволяють легко та швидко передавати трафік між групою абонентів, але паралельно з цим зростає уразливість каналів. Сам принцип дії Wi-Fi демонструє, наскільки легко перехопити ту чи іншу інформацію або здійснити атаку при наявності необхідного обладнання. Головна причина уразливості безпроводових мереж криється в обміні пакетами даних за допомогою радіохвиль. Саме ця технологія дає зловмисникам можливість працювати в будь-якій точці, де сигнал залишається фізично доступним. Якщо мережа не захищена, рано чи пізно до неї спробує приєднатися сторонній користувач. Швидше за все, це буде навіть не зловмисник: дуже часто смартфони та планшети підключаються до відкритих бездротових мереж в автоматичному режимі. Якщо ж незваний гість спробує відкрити кілька сайтів або завантажити на телефон новий додаток, цього складно буде не помітити, адже витрата трафіку збільшиться. Але буде гірше, якщо новий користувач

почне користуватися нелегальними ресурсами. Захист від несанкціонованих підключень — одна з першорядних налаштувань безпеки безпроводових мереж. Окрім зайвих користувачів в безпроводових мережах часто зустрічаються і більш небезпечні користувачі — хакери. Вони можуть зламати Wi-Fi і поміняти існуючі налаштування, щоб ніхто більше не міг увійти в мережу, перехопити чужий трафік з метою використання конфіденційної інформації або використовувати з'єднання для організації нових атак: деякі методи проникнення настільки прості, що скористатися ними може кожен. В таких випадках стандартний пароль не допоможе: параметри безпеки безпроводових мереж для захисту від хакерів повинні бути більш складними і надійними. Ідеальний варіант це наявність IPS запобігання вторгнень.

Через те, що область між кінцевими точками мережі Wi-Fi абсолютно не контролюється, зловмисники, що знаходяться в безпосередній близькості від неї, можуть без великих перешкод приєднатися до неї, що не можна сказати про проводові мережі. Для цього вони використовують спеціальне обладнання та особливі алгоритми, в результаті чого захиститися від виникаючих загроз стає набагато складніше. Найбільш поширена загроза для безпроводових мереж, створювана анонімними хакерами — це перехоплення сигналу та дешифрування інформації, що передається по обраному каналу інформації. Прилади, які використовуються для цього, часто не складніше стандартних роутерів, проте, прослуховування дуже важко зареєструвати, а перервати навіть ще важче. Крім того, хакери користуються підсилювачами і антенами, що дозволяють їм перебувати на значній відстані від мережі. Але якщо перехоплення небезпечне лише перехопленням даних, то повною паралізацією мережі загрожує DOS-атака або заглушення станції. Запобігти і зупинити відмову в обслуговуванні практично неможливо, а наслідки його дуже серйозні. Усі комунікації в конкретній мережі стають відключеними, і зв'язок між терміналами безпроводової мережі переривається [17].

Зловмисники можуть завдати шкоди мережі наступними методами:

— Збір інформації про канали зв'язку для планування і проведення будь-яких дій;
— Організація помилкових точок доступу, необхідних для збору даних завдяки яким здійснюється підключення до мережі;
— Атака принципом DOS. У всій мережі, на базових, клієнтських стадіях виникає високе перевантаження, в результаті відключається вся комунікація;
— Руйнування конфіденційності і цілісності з'єднання методом MITM.

Повний захист безпроводової мережі досягається при комплексному підході до вирішення проблеми. Рівень безпеки залежить від налаштувань, заданих адміністраторами для точки доступу. Один з найважливіших параметрів — режим доступу до мережі. Режими, в яких відбувається функціонування, діляться на 2 види: відкритий і закритий. Закритий — надійний, так як в цьому випадку підключитися до мережі вийде, тільки якщо ввести пароль. Існують такі стандарти захисту мережі [18]:

— WPA;
— WEP;
— WPA2;
— WPA3.

4.2 Дослідження стандартів захисту мережі.

Усього існує чотири найпопулярніші стандарти захисту WPA, WEP, WPA2 та WPA3. Усі ці стандарти більш-менш відомі спеціалістам з телекомунікацій, окрім останнього стандарту WPA3, але перш ніж говорити про те, що нового в цьому стандарті, слід коротко пройтися по попереднім протоколам, починаючи з WEP. Всі існуючі протоколи безпеки безпроводових

мереж — це в тій чи іншій мірі надбудови над своїми попередниками. До того ж, WEP досі достатньо рідко, але використовується та згадати про його не буде зайвим. Безпека WEP забезпечується майже тими ж методами, що і захист в проводових мережах. Що є не дуже ефективним. Якби злочинець хотів перехопити трафік у мережі на фізичному рівні, то йому довелося б проникнути до будівлі, де розташовується мережа, а у випадку з точками доступ з стандартом WEP потрібно всього лише знаходитися в зоні прийому сигналу. Для шифрування трафіку WEP використовується ключовий потік, який виходить з змішування пароля і вектора ініціалізації (IV).

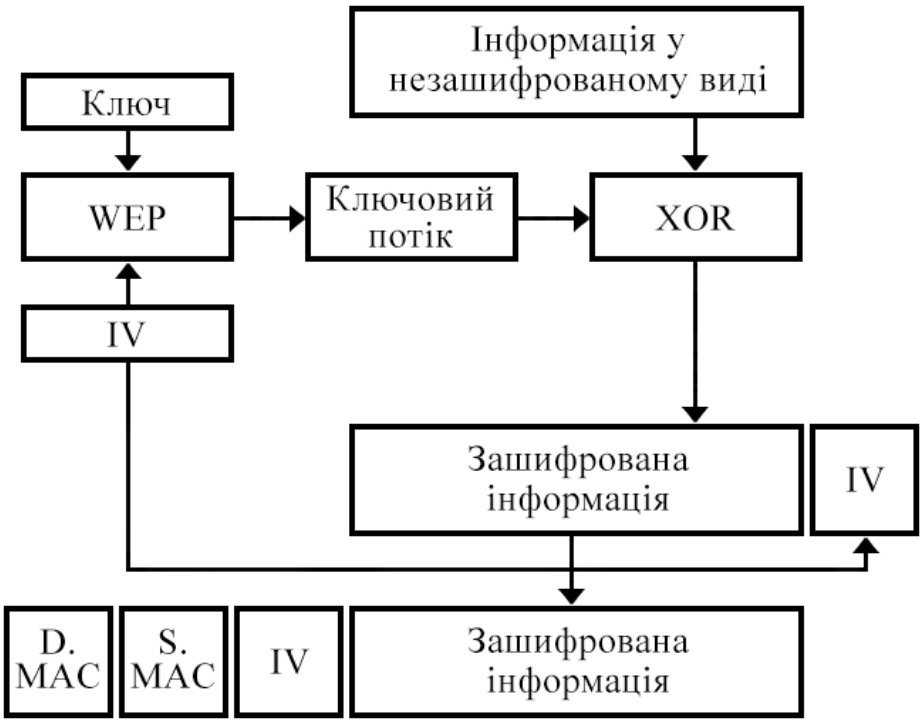


Рисунок 4.1 — Формування шифрованого кадру у протоколі WEP

Вектор ініціалізації у протоколі стандарту безпеки WEP — це постійно змінне 24-бітове число. Може скластися враження, що через постійні зміни ключового потоку підібрати пароль стає неможливо, але цей метод шифрування в сукупності з можливістю перехоплювати пакети виявився слабким місцем стандарту WEP. З ростом обчислювальних потужностей

персональних комп'ютерів довжина вектору ініціалізації стала недостатньою. Якщо довго збирати фрейми, то можна отримати такі, для яких вектор ініціалізації буде однаковим. Таким чином, незалежно від складності ключа розкрити будь-яку передачу стало можливо після статистичного аналізу достатньої кількості перехоплених пакетів (кілька десятків тисяч, що досить мало для активно використовується мережі). Поступово час злому WEP досягає хвилини [19].

Для вирішення проблеми альянс Wi-Fi запропонував надбудову над WEP, яка дозволяла усунути уразливості без заміни обладнання. Першою ідеєю була зміна ключів. Були зібрані всі існуючі на той момент розробки, які ставилися до стандарту IEEE 802.11i, і на їх базі розроблено стандарт WPA. Його основою став протокол TKIP. Він значно посилював WEP за допомогою дворівневої системи векторів ініціалізації. Ідея роботи алгоритму дуже проста. Для кожного нового фрейму зростає значення молодшого вектора ініціалізації (як і раніше в стандарті WEP), але після проходження всіх комбінацій збільшується значення старшого вектора ініціалізації і генерується новий ключ. При зміні ключа база статистики для злому просто не встигає набратися.

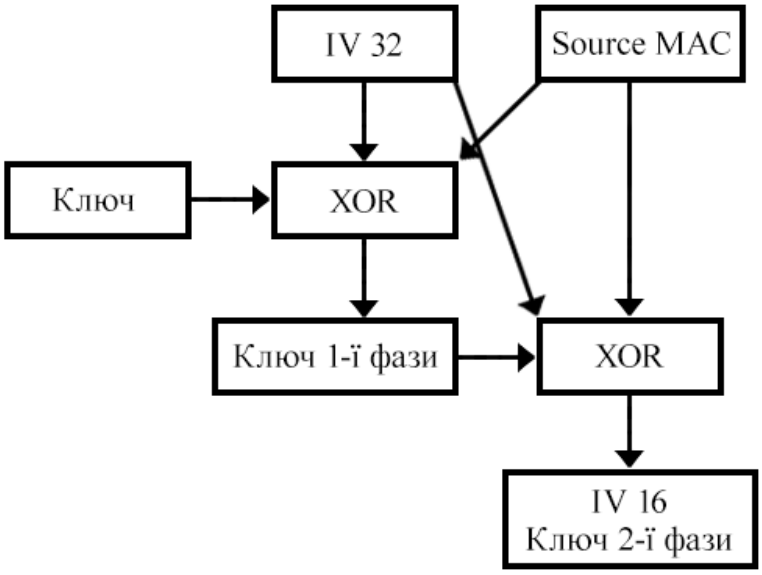


Рисунок 4.1 — Формування шифрованого кадру у протоколі WPA

Іншим нововведенням в WPA стала технологія WPS, яка дозволяє безпроводовим пристроям спрощено отримувати доступ до точки доступу за умови фізичного доступу до маршрутизатора. Ця технологія і стала першою вразливістю стандарту безпеки WPA. Ще одна цікава уразливість ховалася особливо TKIP. Для швидкого усунення критичних вразливостей WEP було введено правило, за яким точка доступу зобов'язана блокувати всі підключення на 60 секунд, якщо вийде зробити підбір ключа. Завдяки цьому захисті стала можлива атака «Michael». Передача зіпсованих пакетів приводила до відключення всієї мережі. Причому на відміну від звичайного DDoS тут достатньо всього двох пакетів для гарантованого виведення мережі з ладу на одну хвилину. Необхідно зауважити, що після виявлення цих вразливостей говорити про злом WPA було ще не зарано. Досить відключити WPS, і перехопити дані буде неможливо. А наявність вибору між комфортом і безпекою не можна назвати критичною уразливістю протоколу. У 2006 році на надійності WPA остаточно поставили хрест уразливості, які дозволяють маніпулювати мережею. Ці атаки засновані на знанні деяких даних в зашифрованих фреймах, наприклад запитів ARP або фреймів для забезпечення QoS. Експлоїт дозволяє читати дані, що передаються від точки доступу клієнтської машині, а також передавати підроблену інформацію на клієнтську машину. Для реалізації цієї атаки необхідно, щоб в мережі використовувався QoS.

До 2006 року все у багатьох безпроводових пристроях було реалізовано стандарт захисту WPA2, але великої паніки злом його попередника не викликав. Кардинальною відзнакою WPA2 від WPA стало індивідуальне шифрування даних кожного користувача. На додачу він використовував надійніший алгоритм шифрування — AES. Довгий час основними методами злому маршрутизаторів, які працювали по WPA2, був злом PIN-коду при підключенні через WPS або перехоплення рукостискання і підбір ключа

методом підбору «грубою силою». Забезпечити себе можна було, відключивши WPS і встановивши досить надійний пароль. Тому до недавнього часу WPA2 вважався надійним і всіх влаштовував. Але, у жовтні 2017 року було опубліковано опис KRACK — засіб злому мереж Wi-Fi, що використовують WPA2. З цього моменту експерти стали вважати протокол WPA2 ненадійним.

У жовтні 2017 року було опубліковано вразливість у стандарті WPA2. І через це шуму стало набагато більше. Новий метод злому назвали атакою з переустановлення ключа — key reinstallation attack, або скорочено KRACK. Атака працює проти всіх сучасних мереж Wi-Fi, в залежності від конфігурації мережі також існує можливість маніпулювання даними. Реалізувати атаку можна, впливаючи на чотиристороння рукостискання протоколу WPA2. Такий хендшейк відбувається, коли клієнт приєднується до захищеної мережі, він підтверджує, що клієнт і точка доступу мають загальні облікові дані. Один з етапів цього процесу — узгодження нового ключа шифрування для всього майбутнього трафіку між клієнтом і мережею. Не будемо зупинятися на великій кількості ключів, які беруть участь в чотирибічному рукостисканні. Першим і другим рукостисканням маршрутизатор і клієнт обмінюються загаданими ними випадковими числами ANonce і SNonce і з їх допомогою обчислюють ключ сесії. Після отримання третього пакета рукостискання клієнт встановлює ключі шифрування і обнуляє лічильник інкремента пакетів nonce. Четвертим рукостисканням клієнт відправляє до маршрутизатора інформацію про те, що ключі встановлені і можна починати обмін даними. Атака реалізується наступним методом. Спочатку зловмисникові необхідно викрасти третій пакет рукостискання. Цей пакет зловмисник ретранслює клієнту, що призводить до переустановлення того ж ключа і обнулення лічильника інкремента пакетів nonce. Лічильник nonce безпосередньо бере участь у створенні ключового потоку, за допомогою якого шифруються пакети, що відправляються між клієнтом і маршрутизатором. Зміна nonce при обміні трафіком гарантує формування абсолютно різних ключових потоків для всіх переданих пакетів.

Але в результаті атаки наступний після переустановлення ключа пакет, що відправляється клієнтом, буде зашифрований тим же ключовим потоком, яким був зашифрований перший пакет та це повертає нас до тих же проблем, які були у WEP.

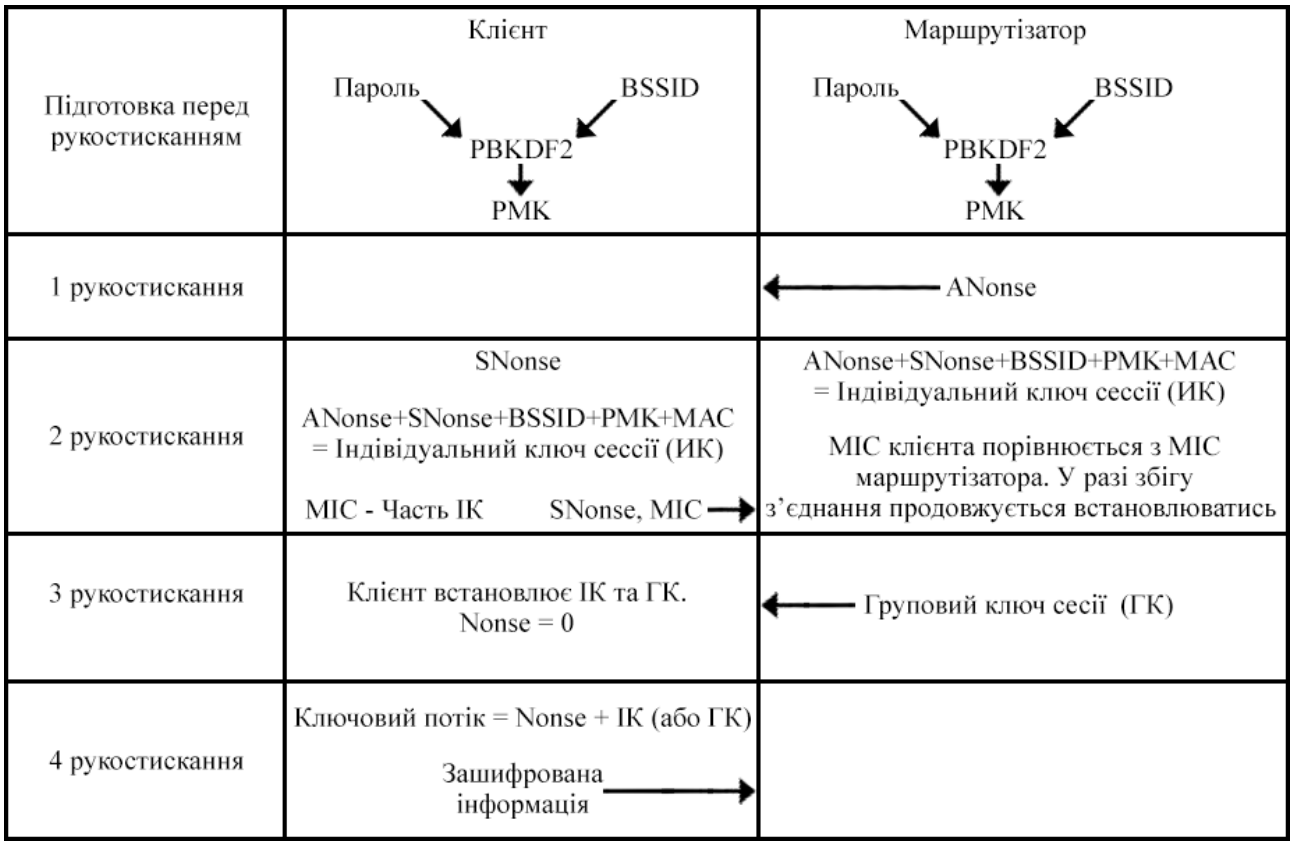


Рисунок 4.3 — Процес чотиристоронього рукостискання

У 2010 році була знайдена уразливість, відома під кодовою назвою hole196, це означає, що на 196-й сторінці стандарту 802.11 знайшлася інформація про те, що для всіх авторизованих в мережі користувачів при широкомовних запитах використовується однаковий ключ шифрування. Завдяки hole196 стали можливими давно відомі атаки ARP/DHCP Spoofing. Уразливість свого часу наробила досить шуму, але назвати її особливо критичною було не можна. Чому? По-перше, перш ніж вести атаку, потрібно

було авторизуватися в мережі. По-друге, ця вразливість лікується застосуванням файрволу.

27 червня 2018 року альянс Wi-Fi оголосив про закінчення розробки нового стандарту безпеки — WPA3. Це одночасно і новий протокол безпеки, і назва відповідної програми сертифікації. Перш ніж на тому чи іншому обладнанні з'явиться назва «WPA3», йому необхідно буде пройти величезну кількість тестів — це гарантує коректну роботу з іншими пристроями, які отримали ту ж назву. З точки зору користувача стандарт WPA3 можна назвати і протоколом безпеки, але мається на увазі під цим не апаратна реалізація, а відповідність нормативам [20].

Розробники WPA3 спробували усунути концептуальні недоробки, які спливли з появою KRACK. Новий стандарт, як і у всіх попередніх випадках, заснований на технологіях його попередника. В анонсі WPA3 представники альянсу Wi-Fi говорили про застосування чотирьох нових технологій. Але в підсумку лише одна з них стала обов'язковою для реалізації виробниками. Оскільки ключова вразливість ховалася в чотирибічному рукостисканні, в WPA3 додалася обов'язкова підтримка більш надійного методу з'єднання — SEA, також відомого як Dragonfly. Технологія SEA (Simultaneous Equals of Authentication) вже застосовувалася в mesh-мережах і описана в стандарті IEEE 802.11s. Вона заснована на протоколі обміну ключами Діффі-Хеллмана з використанням кінцевих циклічних груп. SEA відноситься до протоколів типу PAKE і надає інтерактивний метод, відповідно до якого дві і більше сторони встановлюють криптографічні ключі, засновані на знанні пароля однією або декількома сторонами. Результуючий ключ сесії, який отримує кожна зі сторін для аутентифікації з'єднання, вибирається на основі інформації з пароля, ключів і MAC-адрес обох сторін. Якщо ключ однієї зі сторін виявиться скомпрометований, це не спричинить компрометації ключа сесії. І навіть дізнавшись пароль, злочинець не зможе розшифрувати пакети [21].

Ще одним нововведенням WPA3 буде підтримка PMF (Protected Management Frames) для контролю цілісності трафіку. Але в майбутньому підтримка PMF стане обов'язковою і для WPA2. Не потрапили в сертифікацію WPA3 програми Wi-Fi Easy Connect і Wi-Fi Enhanced Open. Wi-Fi Easy Connect дозволяє реалізувати спрощену настройку пристроїв без екрану. Для цього можна використовувати інший, більш сучасний пристрій, вже підключений до безпроводової мережі. Наприклад, параметри мережі для датчиків і розумних речей домашнього вжитку можна буде задавати зі смартфона, сфотографувавши QR-код на корпусі девайса. Easy Connect заснований на застосуванні аутентифікації по відкритих ключах (в QR-коді передається відкритий ключ) і може використовуватися в мережах з WPA2 і WPA3. Ще одна приємна особливість Wi-Fi Easy Connect — можливість заміни точки доступу без необхідності перенастроювати всі пристрої. Wi-Fi Enhanced Open має на увазі шифрування всіх потоків даних між клієнтом і точкою доступу. Ця технологія дозволить захистити приватність користувача в публічних мережах, де не потрібно аутентифікація. Для генерації ключів в таких мережах буде застосовуватися процес узгодження з'єднання, що реалізовується розширенням Opportunistic Wireless Encryption. Підтримка обох технологій не обов'язкова для сертифікації по WPA3, але виробник може при бажанні сам включити їх підтримку в продукт. Як і в WPA2, в WPA3 передбачено два режими роботи: WPA3-Personal і WPA3-Enterprise.

— WPA3-Personal забезпечить надійний захист, особливо якщо користувач задав стійкий пароль, який не можна отримати словниковим перебором. Але якщо пароль не зовсім тривіальний, то повинно допомогти нове обмеження на число спроб аутентифікації в рамках одного рукостискання. Також обмеження не дозволить підбирати пароль в офлайн режимі. Замість ключа PSK в WPA3 реалізована технологія SEA.

— WPA3-Enterprise має на увазі шифрування на основі як мінімум 192-розрядних ключів, які відповідають вимогам CNSA (вони вироблені комітетом NSS для захисту урядових, військових та промислових мереж). Для аутентифікованного шифрування рекомендовано застосування 256-розрядних ключів GCMP-256, для передачі і підтвердження ключів використовується HMAC з хешамі SHA-384, для узгодження ключів і аутентифікації - ECDH і ECDSA з 384-розрядними еліптичними кривими, для захисту цілісності кадрів — протокол BIP- GMAC-256.

Поки немає офіційної інформації про пристрої, які зможуть в майбутньому отримати підтримку WPA3. Навряд чи варто сподіватися і на те, що в багатьох роутерах WPA3 з'явиться після апдейта прошивки. У теорії це можливо, але тоді виробникам доведеться сертифікувати старі пристрої. Швидше за все, робити цього вони не будуть і краще витратити ресурси на випуск нових моделей. На офіційному сайті Альянсу Wi-Fi вже опублікований список пристроїв з підтримкою WPA3. Однак наявність такого списку означає, що до появи WPA3 залишилося рівно стільки часу, скільки необхідно для інтеграції протоколу в нові пристрої. За прогнозами альянсу Wi-Fi, очікується, що пристрої з підтримкою WPA3 поширяться на ринку в 2019 році разом з пристроями з підтримкою Wi-Fi-802.11ax (або Wi-Fi 6 відповідно до нової схеми найменування) [22].

Отже, виходячи з досліджень розглянутих вище, можна зробити висновки, що WPA3 є самим новим та сучасним стандартом безпеки безпроводових мереж і було б логічно запропонувати використовувати саме цей його, але, він на ринку телекомунікацій лише два роки і багато не усі пристрої підтримують цей стандарт. Обрана точка доступу має підтримку стандарту WPA3, але для коректної роботи цей стандарт потрібен також підтримувати і пристрій, який підключається до точки доступу. Тому, пропонується використовувати режим захисту WPA2, який застосовується на

пристроях вже понад 15 років, та має підтримку майже усіх пристроїв. Але, обрані точки доступу які мають стандарт IEEE 802.11ax готові працювати з механізмом захисту WPA3, тому, у майбутньому, коли цей механізм набуде більшої популярності то буде підтримуватися на клієнтських пристроях.

4.3 Розгляд рекомендованого механізму безпеки мережі.

Окрім того, що було рекомендовано використовувати стандарт захисту мережі WPA2, слід трохи ознайомитися з його функціями та принципом роботи, а також розглянути існуючий у точці доступу Huawei WiFi AX3 механізм безпеки. Для того щоб підключитися до мережі з захистом WPA2, клієнт повинен аутентіфікуватися на головному сервері. Аутентифікацію можна пройти за допомогою доменного пароля, клієнтського сертифіката, тощо. Шифрування організовано за алгоритмом AES. Ключ шифрування динамічний, індивідуальний для кожного клієнта, генерується в момент аутентифікації на сервері. Цей ключ може підлягати періодичному оновленню по ходу роботи без розриву з'єднання. Процес підключення клієнта до бездротової мережі коротко можна описати так. При підключенні дані клієнта передаються на точку доступу за участю протоколу 802.11. Далі інформація відправляється на сервер, де відбувається аутентифікація клієнта: сервер перевіряє, чи є в його списках такий клієнт із зазначеним логіном і паролем, і чи можна його підключати. Після успішної аутентифікації точка доступу підключає клієнта в мережу [23].

Також, рекомендована до використання точка доступу має свої власні механізми захисту. У чотирьох ядерний процесор маршрутизатора Huawei WiFi

AX3 з можливостями TEE (середовище безпечного виконання) і мікроядром Harmony вбудовано незалежну зону безпеки, що гарантує захист ваших даних на програмному та апаратному рівні [24]. Маршрутизатор отримав сертифікат CC EAL5, що означає безпечну роботу в комерційному середовищі, а отже, гарантує високий рівень захисту ваших пристроїв. Сертифікат EAL5 дозволяє розробнику отримати максимальну впевненість від проектування безпеки безпроводової мережі, заснованого на строгих практиках комерційної розробки, підтримуваних помірним застосуванням спеціальних методів проектування безпеки. Таким чином, EAL5 застосовується в тих обставинах, коли розробникам або користувачам потрібен високий рівень незалежно гарантованої безпеки при запланованій розробці і потрібен строгий підхід до розробки без невиправданих витрат, пов'язаних з використанням спеціальних методів проектування безпеки [25].

Висновки до розділу 4

У четвертому розділі було досліджено механізми безпеки для безпроводової мережі. Безпека безпроводових мереж дуже важлива для зберігання персональних даних від доступу для зловмисників, які можуть несанкціоновано приєднатися до мережі, та перехопити дані, що передаються у мережі.

Для організації надійного захисту було проведено дослідження, та розглянуто найпопулярніші протоколи захисту: WEP, WPA, WPA2 та WEP3. Після проведення досліджень та порівняння переваг та недоліків кожного з цих протоколів, було рекомендовано до використання протокол WPA2.

Стандарт захисту WPA2, який було рекомендовано для використання у безпроводовий мережі, що проектується підтримується обраними точками доступу, та є найбільш популярним та підтримуваним пристроями. Але не

виключено використання стандарту WPA3 у майбутньому, коли він набуде більшою поширеності на пристроях користувачів.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКИ ПРИ НАДЗВИЧАЙНИХ СІТУАЦІЯХ НА ПІДПРИЄМСТВІ

5.1 Характеристика умов праці.

Одним з важливих відділів лікарні є відділ моніторингу мережі. Труд працівників цього відділу дуже інтенсивний та напружений, який потребує значні затрати розумової, емоційної та фізичної енергії. Працівники тісно пов'язані з комп'ютерною технікою. При роботі з комп'ютерною технікою людина піддається впливу багатьох шкідливих та небезпечних факторів: електромагнітних полів (діапазон радіочастот ВЧ, УВЧ, СВЧ), інфрачервоного та іонізуючого випромінювань, шуму та вібрації, статичної електрики та ін.

Робота з комп'ютером характеризується значною розумовою напруженістю та нервово-емоційним навантаженням операторів, високою напруженістю зорової праці та достатньо великим навантаженням на мишці рук при роботі з клавіатурою.

В процесі роботи з комп'ютером необхідно дотримуватися правильного режиму праці та відпочинку.

Ці фактори можуть привести до професійних захворювань таких, як комп'ютерна алергія, радіохвильова хвороба, захворювання шкіри, синдром Сіка, язва шлунку, комп'ютерний зоровий синдром, стрес, кистьовий тунельний синдром.

Діяльність працівників відділу:

- моніторинг активного обладнання мережі, виявлення відмов та аварійних ситуацій на обладнанні;
- аналіз виникаючих аварій;
- організація оперативних дій по усуненню аварій;
- формування звітів;

- робота, за потребою, з оргтехнікою (факс, принтер, копіювальний апарат) та Інтернетом.

Відділ моніторингу мережі розташовується на першому поверсі лікарні №1 в приміщенні з установленою технікою згідно з СНиП II-90-81 «Виробничі будівлі промислових підприємств», загальна площа приміщення становить 30 м², а загальний обсяг – 90 м³.

5.2 Вимоги до виробничих приміщень.

5.2.1 Освітлення.

Правильно спроектоване та виконане освітлення покращує умови зорової роботи, знижує втому, сприяє підвищенню продуктивності труда, благотворно оказує вплив на виробниче середовище, надаючи позитивний психологічний вплив на працівника, підвищує безпеку праці та знижує травматизм.

Недостатнє освітлення призводить до напруження зору, послаблює увагу, призводить до передчасної втоми. Надмірна яскравість викликає осліплення, роздратування та різь в очах. Неправильний напрям освітлення на робочому місці може створювати різкі тіні, відблиски, дезорієнтованість працівника. Всі ці причини можуть призвести до нещасного випадку або профзахворюванням, цьому важливий правильний розрахунок освітлення.

Згідно СНиП II-4-79 в приміщенні необхідно застосовувати систему комбінованого освітлення.

При виконанні робіт категорії високої зорової точності (найменший розмір об’єкта розрізнення 0,3…0,5 мм) величина коефіцієнта природнього освітлення (КПО) повинна бути не нижче 1,5%, а при зорової роботі середньої точності (найменший розмір об’єкта розрізнення 0,5…1,0 мм) КПО повинен

бути не нижче 1%. В якості джерел штучного освітлення зазвичай використовуються люмінесцентні лампи типу ЛБ або ДРЛ, які попарно об'єднуються до світильників, які повинні розташовуватися над робочими поверхнями рівномірно.

Вимоги до освітлення у приміщеннях, де встановлені комп'ютерна техніка, наступні: при виконанні зорових робіт високої точності загальна освітленість повинна складати 300 лк, а комбінована – 750 лк; аналогічні вимоги при виконанні робіт середньої точності – 200 и 300 лк відповідно.

Крім того все поле зору повинно бути освітлене достатньо рівномірно – це основна гігієнічна вимога. Іншими словами, степінь освітлення приміщення та яскравість екрану комп'ютера повинні бути приблизно однаковими, тому що яскраве світло у районі периферійного зору значно збільшує напругу очей та, як наслідок, призводить до їх швидкої втоми.

5.2.2 Параметри мікроклімату.

Параметри мікроклімату можуть змінюватися в широких межах, в той час як необхідною умовою життєдіяльності людини є підтримка постійності температури тіла завдяки терморегуляції, тобто здатності організму регулювати віддачу тепла до навколишнього середовища. Принцип нормування мікроклімату – створення оптимальних умов для теплообміну тіла людини з навколишнім середовищем.

Комп'ютерна техніка є джерелом суттєвих тепловиділень, що може призвести до підвищення температури та зниженню відносної вологи в приміщенні. У приміщенні, де встановлені комп'ютери, повинні дотримуватися певні параметри мікроклімату. В санітарних нормах СН 245-71 встановлені величини параметрів мікроклімату, які створюють комфортні умови. Ці норми встановлюються залежно від пори року, характеру трудового процесу та характеру виробничого приміщення.

Об’єм приміщень, в яких розташовані робочі місця працівників відділу моніторингу, не повинен бути менш ніж 19,5 м³/людину з урахуванням максимального числа одночасно працюючих за зміну

Таблиця 5.1 – Параметри мікроклімату для приміщення з комп’ютерами

Пора року	Параметри мікроклімату	Величина
Холодна	Температура повітря	22…24 ºС
	Відносна вологість	40…60 %
	Швидкість руху повітря	До 0,1 м/с
Тепла	Температура повітря	23…25 ºС
	Відносна вологість	40…60 %
	Швидкість руху повітря	0,1…0,2 м/с

Таблиця 5.2 – Норми подачі свіжого повітря в приміщення, де розташована комп’ютерна техніка

Характеристика приміщення	Об’ємні витрати свіжого повітря, що подається в приміщенні м³/на одну людину в годину
Об’єм до 20 м³ на людину	Не менш ніж 30
20…40 м³ на людину	Не менш ніж 20
Більш ніж 40 м³ на людину	Природня вентиляція

Для забезпечення комфортних умов використовуються як організаційні методи (раціональна організація проведення робіт в залежності від пори року та доби, чергування праці та відпочинку), так й технічні засоби (вентиляція, кондиціювання повітря, опалювальна система).

5.2.3 Шум та вібрація.

Шум погіршує умови праці, надає шкідливий вплив на організм людини. Люди, що працюють в умовах тривалого шумової дії відчувають роздратованість, головний біль, запаморочення, погіршення пам’яті, підвищення втоми, зниження апетиту, біль у вухах та ін. Такі порушення в роботі ряду органів та систем організму людини можуть визвати негативні

зміни в емоційному стані людини аж до стресових. Під дією шуму знижується концентрація уваги, порушуються фізіологічні функції, з'являється втома у зв'язку з зростанням енергетичних затрат та нервово – психічними напругами, погіршується речова комутація. Все це знижує працездатності людини та його продуктивність, якість та безпеку праці. Тривала інтенсивна дія шуму [більш ніж 80 дБ(А)] на слух людини призводить до його часткової або повної втрати.

Рівень шуму на робочому місці працівника відділу моніторингу не повинно перевищувати 75 дБА. Для зниження рівня шуму стіни та стелі приміщень, де встановлена комп'ютерна техніка, можуть бути облицьовані звукопоглинальними матеріалами. Рівень вібрації в приміщеннях таких відділів може бути знижені шляхом встановлення обладнання на спеціальних віброізоляторів.

Таблиця 5.3 – Граничні рівні звуку на робочих місцях, дБ

Категорія напруженості праці	Категорія важкості праці			
	I. Легка	II. Середня	III. Важка	IV. Дуже важка
I. Мало напружений	80	80	75	75
II. Помірно напружений	70	70	65	65
III. Напружений	60	60	-	-
IV. Дуже напружений	50	50	-	-

5.2.4 Електромагнітне та іонізуюче випромінювання.

Максимальний рівень рентгенівського випромінювання на робочому місці взагалі не перевищує 10 мкбер/г, а інтенсивність ультрафіолетового та інфрачервоного випромінювань від екрану монітору лежить у межах 10…100 мВт/м².

Для зниження дії цих видів випромінювань рекомендується застосовувати монітори з пониженим рівнем випромінювань, встановлювати захисні екрани, а також дотримуватися регламентованих режимів праці та відпочинку.

Таблиця 5.4 – Допустимі значення параметрів неіонізуючих електромагнітних випромінювань (згідно з СанПиН 2.2.2.542-96)

Параметр	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50 см від поверхні монітору	10 В/м
Напруженість магнітної складової електромагнітного поля на відстані 50 см від поверхні монітору	0,3 А/м
Напруженість електростатичного поля не повинна перевищувати для дорослих користувачів	20 кВ/м

5.3 Режим праці.

Якщо не дотримуватися правил режиму праці, відзначаються значні напруги зорового апарату з появою скарг на незадовільність роботою, головний біль, роздратованість, порушення сну, втома та біль в очах, в попереку, в області шиї та рук.

Час перерв наведено при дотриманні СанПин 2.2.2 542 – 97. При невідповідності фактичних умов труда потребам санітарних правил та норм час регламентованих перерв потрібно збільшити на 30%.

Згідно з СанПиН 2.2.2 546-96 всі види трудової діяльності, пов’язані з використанням комп’ютера, поділяються на три групи:

- група А: робота пов’язана з зчитування інформації з екрану ;
- група Б: робота пов’язана з вводом інформації;
- група В: творча робота в режимі діалогу.

Ефективність перерв підвищується при співвідношенні з виробничою гімнастикою або організації спеціального приміщення для відпочинку персоналу з комфортними м’якими меблями, акваріумом, зеленою зоною та ін.

Таблиця 5.5 – Час регламентованих перерв при роботі з комп’ютерною технікою

Категорія роботи з комп’ютерною технікою	Рівень навантаження за робочу зміну при видах роботи з монітором			Сумарний час регламентованих перерв у хвилинах	
	Група А, кількість символів	Група Б, кількість символів	Група В, годин	8 – годинна зміна	12 – годинна зміна
I	До 20 000	До 15 000	До 2,0	30	70
II	До 40 000	До 30 000	До 4,0	50	90
III	До 60 000	До 40 000	До 6,0	70	120

5.4 Планування відділу моніторингу.

Відповідно до наведеного аналізу рекомендується розташувати меблі наступним чином

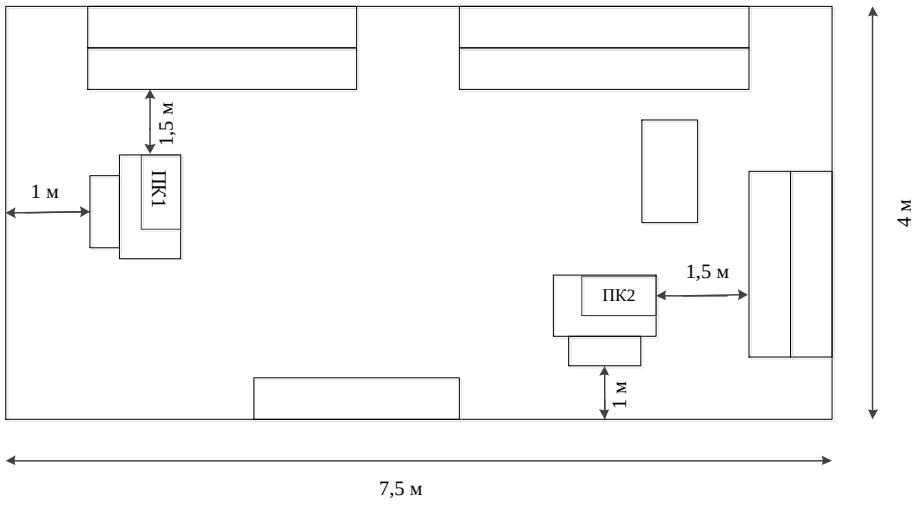


Рисунок 5.1 – Розташування робочих місць відділу моніторингу згідно ГОСТ

Облаштованість робочих місць відповідає вимогам санітарних норм та в приміщенні площею 30 м² та об’ємом 90 м³ можна розташовувати два робочих місць з ПК

5.5 Пожежна безпека.

Найважливішою умовою роботи будь-якого підприємства є дотримання правил пожежної охорони.

У приміщенні відділу основні міри для забезпечення пожежної безпеки визначає Інструкція про заходи пожежної безпеки для службових приміщень. Вона є обов’язковою для виконання всіма співробітниками.

В інструкції про засоби пожежної безпеки для службових приміщень забороняється:

- улаштовувати тимчасові електромережі, застосовувати саморобні плавкі вставки в запобіжниках, прокладати електричні проводи безпосередньо по пальній основі, експлуатувати світильники зі знятими ковпаками (розсіювачами), використовувати саморобні подовжувачі, що не відповідають вимогам Правил пристрою електроустановок;
- пристосовувати вимикачі, штепсельні розетки для підвішування одягу й інших предметів, обгортати електролампи і світильники, заклеювати ділянки електромережі пальною тканиною, папером;
- використовувати побутові електрокип'ятильники, чайники тощо без незаймистих підставок, залишати без нагляду включеними в електромережу кондиціонери, комп'ютери, рахункові і друкарські машинки і т.п.;
- захаращувати підступи до засобів пожежогасіння, використовувати пожежні крани, рукави і пожежний інвентар не по призначенню, зберігати документи, різні матеріали, предмети й інвентар у шафах (нішах) інженерних комунікацій;
- курити (крім спеціально відведених для цього адміністрацією місць, позначених написом «Місце для паління» і забезпечених урною чи попільницею з матеріалу, що не горить), проводити зварювальні й

інші вогневі роботи без оформлення відповідного дозволу, застосовувати легкозаймисті рідини.

По закінченню роботи необхідно:

- оглянути приміщення, переконатися у відсутності порушень, що можуть спричинити пожежу;
- відключити освітлення, електроживлення приладів і устаткування.

Електромережі, електроприлади і апаратура повинні експлуатуватися тільки у справному стані. У випадку виявлення ушкоджень електромереж, вимикачів, розеток ті інших електровиробів варто негайно відключити їх і вжити необхідних заходів до приведення їх в пожежобезпечний стан.

5.6 Безпека при надзвичайних ситуаціях на підприємстві.

Об’єктом забезпечення на предмет визначення надзвичайних небезпек та їх наслідків є службове приміщення підприємства зв’язку . Однією із вірогідних загроз може бути раптове виникнення пожару внаслідок короткого замикання в електромережах або розрядів статистичної електрики, що може привести до пошкодження і руйнування будівлі, устаткування, комунікацій, виділення токсичних продуктів горіння.

Тому розроблено оперативний план гасіння пожежі, який визначає порядок дії персоналу при пожежі, порядок її гасіння в електроустановках, взаємодію з власним складом пожежних підрозділів, а також застосування схем и засобів пожежогасіння з урахуванням заходів безпеки.

Підприємство повинно бути обладнаним мережею протипожежного водо забезпечення, установками виявлення та гасіння пожеж відповідно вимогам нормативно-технічних документів. Кожний працівник повинен чітко знати та виконувати вимоги ППБ та протиаварійний режим на об’єкті, уміти користуватися наявними вогнегасниками, іншими первинними засобами пожежогасіння і знати місце їхнього перебування.

Меблі й устаткування повинні розміщатися таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу з приміщення (шириною не менше 1 м). Евакуаційні шляхи і виходи необхідно постійно держати вільними, нічим не захаращувати. Засоби протипожежного захисту в приміщеннях потрібні триматися у справному стані.

У випадку виявлення пожежі слід:

- негайно повідомити державну пожежну охорону за телефоном «101», вказати при цьому адресу, кількість поверхів, місце виникнення пожежі, наявність людей, своє прізвище;
- повідомити про пожежу керівництву, а в нічний час черговому охоронцю.

У разі можливості почати гасіння пожежі наявними засобами, організувати зустріч пожежних підрозділів.

При виникненні пожежі у початковій стадії її розвитку випромінюється тепло, токсичні продукти згоряння, імовірні руйнування будівельних споруд. Тому слід як можна швидше провести евакуацію людей із палаючої будівлі. Показником ефективності евакуації є час, протягом якого працівники можуть при потрібності залишити окремі приміщення і будівлю в цілому. Безпека евакуації досягається тоді, коли час евакуації не перевищує час настання критичної фази розвитку пожежі, тобто часу від початку пожежі до досягнення граничних для людини впливів факторі пожежі (критичних температур, ступені задимлення, зниження концентрації кисню и т.п.). Число евакуаційних виходів повинно бути не менш двох. Вони повинні розташовуватися розосереджено.

Двері на шляхах евакуації повинні відкриватися у напрямку виходу із будівлі (приміщення).

У кожному приміщенні на видному місці повинен бути вивішений план евакуації при пожежі.

При пожежі обов'язково необхідно враховувати небезпечні чинники і механізм їх дії на людину.

При виникненні пожежі, після виклику пожежної охорони, необхідно попередити про це усіх, хто знаходиться поруч, після чого евакуюватися самому і по можливості допомогти евакуюватися іншим, особливо особам літнього віку і дітям, попереджаючи при цьому виникнення паніки. З метою обмеження циркуляції повітря, яке здатне збільшувати швидкість горіння, покидаючи приміщення, закрийте за собою усі двері, якщо це можливо.

Якщо пожежа виникла в приміщенні над вами і безпосередньої загрози для вас не спостерігається, то бажано виконати заходи по зниженню можливих втрат від води яку проливають при гасінні пожежі. Для цього необхідно відключити всі електроприводи та прикрити їх поліетиленовою плівкою. Значно гірше, якщо пожежа виникла в приміщенні над вами – потрібно оцінити обстановку и якщо є впевненість, що ще не має сильної задимленості з високою температурою, потрібно негайно покинути приміщення, рухаючись до виходу по коридорам і сходовим кліткам.

Користуватися ліфтом категорично забороняється, за винятком ліфтів, які спеціально призначені для транспортування пожежної охорони. Шахта ліфта є шляхом для поширення диму і отруйних продуктів горіння, до того ж при пожежі ліфт часто відключають і можна опинитися в пастці при пожежі.

Якщо ви знаходитеся в приміщенні де немає пожежі, але відрізани вогнем, димом, високою температурою від головних шляхів евакуації, то в першу чергу необхідно заважити доступу диму и продуктів горіння в це приміщення. Для чого необхідно негайно закрити усі щілини у дверях та під ними змоченими водою ганчірками, рушниками, робочими халатами та ін.

Якщо приміщення все ж заповнено димом, необхідно підповзти до вікна, закрити при цьому рот та ніс змоченою тканиною, яка грає роль фільтру та в певної мірі захищає від продуктів горіння.

Рухатись у задимленій зоні поповзом або максимально пригнувшись, необхідно тому що більшість нагрітих газоподібних отруйних речовин та дим збираються у верхній зоні приміщення, окрім цього, в приміщенні при горінні температура на рівні очей людини у 6 разів вище за температуру на рівні полу,

до того ж внизу завжди зберігається більша концентрація кисню. Коли ви опинились біля вікна трохи відкрийте його та дихайте через щілину, очікуючи прибуття пожежників. При їх прибутті негайно зверніть на себе увагу. Ніколи не стрибайте через вікно без відомої на це необхідності (кожний другий стрибок з 4-г поверху при пожежі смертельний).

Висновки до розділу 5

В цьому розділі було розглянуто охорону праці та безпеки життєдіяльності при надзвичайних ситуаціях. Було проведено аналіз умов праці персоналу та заходів для покращення комфорту роботи. Визначили необхідні стандарти освітлення та мікроклімату робочого місця. Розглянуто необхідні дії при пожежній небезпеці та варіанти запобігання надзвичайних ситуацій.

ВИСНОВКИ

У представленому проекті спроектована мережа безпроводового доступу комунального підприємства «Центр первинної медико-санітарної допомоги» Покровської міської ради», розроблено радіомоделювання мережі та досліджено механізми безпеки для надання необхідного захисту для мережі.

У першій главі дипломного проекту звернуто увагу на опис та характеристику об’єкту моделювання та модернізації мережі. Об’єктом для роботи виступає комунальне підприємство «Центр первинної медико-санітарної допомоги» Покровської міської ради. Також було розглянуто класи та стандарти безпроводових мереж і порівняні з попередніми стандартами. Було переглянуто та перерахування трафіку. Було потрібно змоделювати частотне планування, для більш коректної та продуктивної роботи мережі. Мережа необхідна мати надійний захист від атак зловмисників. Отже, треба детально дослідити механізми безпеки, задля запобігання несанкціонованого доступу до мережі комунального підприємства. При проектуванні безпроводової мережі було зроблено розподіл користувачів по класам та розроблена інформаційна модель мережі. Мережа має надавати послуги безпроводового доступу до мережі інтернет.

У другій главі було перераховано та скореговано вимоги до мережі, завдяки чому вдалось з’ясувати, що мережа зазнала помітних змін — кількість прогнозованих абонентів збільшилась, а навантаження на мережу зросло. Були переглянуті стандарти та технології мережі, що проектується — вирішено обрати стандарт IEEE 802.11ax, та були обрані точки доступу — Huawei WiFi AX3.Для наглядного прикладу мережі було розроблено синтез структурної схеми. Після цього була перерахована кількість точок доступу для кожного підприємства та з урахуванням розташування приладів за площею будівель був отриманий результат у 36 точок доступу на кожне підприємство та

перебудовані схеми розміщень кінцевих обладнань. У завершенні підрахунку параметрів було змоделювано зону покриття безпроводової мережі — обрано місця розташування точок доступу за розрахованою кількістю та розміщено їх за площею будівель.

У третьому розділі розроблено радіомоделювання мережі. Було обрано програмне забезпечення Wi-Fi Analyzer для аналізу середовища та розглянуто його головні функції та переваги. Завдяки цьому додатку було проаналізовано середовище трьох будівель де проектується безпроводова мережа, визначено завантаження каналів та кількість пристроїв у мережі. Після аналізу середовища було зроблено радіомоделювання покриття мережі за допомогою додатка Wi-Fi Planner PRO від «D-Link» та за результатом моделювання зроблено висновки, що кількість та розташування точок доступу є оптимальним.

У четвертому розділі було досліджено механізми безпеки для безпроводової мережі для зберігання персональних даних від доступу зловмисників, які можуть несанкціоновано приєднатися до мережі, та перехопити дані, що передаються у мережі. Для організації надійного захисту було проведено дослідження, та розглянуто найпопулярніші протоколи захисту: WEP, WPA, WPA2 та WEP3 та розглянувши переваги та недоліки усіх стандартів було рекомендовано до використання протокол WPA2. Цей протокол є найбільш популярним та підтримуваним пристроями. Але не виключено використання стандарту WPA3 у майбутньому, коли він набуде більшою поширеності на пристроях користувачів.

У четвертому розділі було розглянуто охорону праці та безпеки життєдіяльності при надзвичайних ситуаціях. Було проведено аналіз умов праці персоналу та заходів для покращення комфорту роботи. Визначили необхідні стандарти освітлення та мікроклімату робочого місця. Розглянуто необхідні дії при пожежній небезпеці та варіанти запобігання надзвичайних ситуацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТРИ

1. Тіссен О. С. ДОСЛІДЖЕННЯ ТА МОДЕРНІЗАЦІЯ МЕРЕЖІ БЕЗПРОВОДОВОГО АБОНЕНТСЬКОГО ДОСТУПУ КОМУНАЛЬНОГО ПІДПРИЄМСТВА «ЦЕНТР ПЕРВИННОЇ МЕДИКО-САНІТАРНОЇ ДОПОМОГИ» ПОКРОВСЬКОЇ МІСЬКОЇ РАДИ З УРАХУВАННЯМ МЕХАНІЗМІВ БЕЗПЕКИ / Олександр Сергійович Тіссен. // «ТАК» Телекомунікації, автоматизація, комп'ютерно-інтегровані та інформаційні технології. – 2020. – С. 10–12.
2. Соловйов М.С., Воропаєва В.Я. Забезпечення показників якості в конвергентних мережах GSM/Wi-Fi при впровадженні нових сервісів // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 16 (147). - Донецьк-2009. – 248 с., С. 22-28
3. Шосте покоління Wi-Fi [Електронний ресурс] – Режим доступу до ресурсу: https://www.tp-link.com/ru-ua/wifi6/.
4. Що таке 802.11ax - огляд нового стандарту WI-FI 6 [Електронний ресурс] – Режим доступу до ресурсу: https://www.sit-com.ru/802-11ax-review-wifi6.html#802-11-ax.
5. Основи радіочастотного планування стосовно Wi-Fi Cisco [Електронний ресурс] – Режим доступу до ресурсу: https://blog.telecom-sales.ru/osnovy-radiochastotnogo-planirovaniya-primenitelno-k-wi-fi-cisco/.
6. Теорія телетрафіку: навч. посіб. / В.Я. Воропаєва, В.І. Бессараб, В.В. Турупалов, В.В. Червинський. – Донецьк: ДВНЗ «ДонНТУ», 2011. – 202 с
7. Безпека безпроводових WLAN і WiFi [Електронний ресурс] – Режим доступу до ресурсу: https://wireless-e.ru/wlan/wifi/bezopasnost-wifi/.
8. Методичні рекомендації до курсового проекту за курсом "Проектування засобів та систем телекомунікаційних мереж" для студентів заочної

форми навчання по спеціальності 7.091402 "Телекомунікаційні системи та мережі" / Укл.: доц.. Дегтяренко І.В. - Донецьк: ДонНТУ, 2007.- 43 с.

9. Воропаева В.Я., Литвинов А. А. Методика прогнозирования параметров трафика телекоммуникационных сетей // Вестник НТУ «ХПИ». Сборник научных трудов. Тематический выпуск «Системный анализ, управление и информационные технологии». – Харьков, НТУ «ХПИ». – 2005. - № 54. – 180 с. С. 142 – 147.
10. Воропаева В.Я., Шапо В.Ф. Метод расчета пропускной способности межсетевых экранов в информационных системах предприятий // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 22 (200). - Донецьк, ДонНТУ, 2012. С - 79-84
11. Макаренко В.В. Особенности стандарта беспроводной связи IEEE 802.11ac (Wi-Fi) / Электронные компоненты и системы, №7, 2012. с. 28-35.
12. Воропаєва В.Я. Оцінка показників якості NGN-мереж з урахуванням фрактальності вхідного трафіку. // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 15 (130). - Донецьк-2008. – 214 с. С. 23-29.
13. І.Л. Щербов, В.Я. Воропаєва, Г.А. Вашакідзе алгоритм прийняття ризику з метою забезпечення безпеки ТКС // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 2(27). - Донецьк: ДонНТУ, 2014. - С. 164-173
14. Викулов А. С., Парамонов А. И. Стандарт IEEE 802.11ax и перспективы его применения для интернета вещей // 2-я Международная научно-техническая конференция студентов, аспирантов и молодых ученых «Интернет Вещей и 5G». 2016. С. 38–41.
15. Як використовувати програму Wi-Fi Analyzer [Електронний ресурс] – Режим доступу до ресурсу: https://nastroyvse.ru/programs/review/kak-polzovatsya-programmoj-wi-fi-analyzer.html.

16. Особливості планування радіорелейних систем в мережах мобільного зв'язку / А. І. Семенко, А. А. Шокотько // Вісник Національного університету "Львівська політехніка". Радіоелектроніка та телекомунікації. - 2014. - № 796. - С. 113-118.
17. Защита беспроводных сетей [Електронний ресурс] – Режим доступу до ресурсу: https://xserver.a-real.ru/support/useful/zashchita-besprovodnykh-setey/.
18. Compfixer (2015) Режим безопасности Wi-Fi: WEP, WPA, WPA2. Что лучше? За адресом: http://compfixer.info/wpa-wep/ (13 Листопада 2015)
19. Безопасность WPA3 [Електронний ресурс] – Режим доступу до ресурсу: https://spy-soft.net/wpa3/#_WPA3.
20. Герасимов, Л. WPA3. Смотрим, что нового в следующем стандарте безопасности Wi-Fi, изучаем прошлые / Л. Герасимов // хакер.т :[сайт]. — URL : https://xakep.ru/2018/10/26/wpa3/ (дата обращения: 20.11.2019).
21. Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11. - М: РадиоСофт, 2010, -255 с.
22. Защита при использовании публичных Wi-Fi сетей // SaferVPN [Електронний ресурс]. – Режим доступу : https://www.safervpn.com/ru/what-is-a-vpn/wifi-security
23. Угрозы для беспроводной корпоративной сети WPA2-Enterprise и способы защиты [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/dataline/blog/327542/.
24. HUAWEI WiFi AX3 (Quad-core) [Електронний ресурс] – Режим доступу до ресурсу: https://consumer.huawei.com/ua/routers/ax3-quad-core/
25. Исследование защищенности Wi-Fi сетей в г. Киеве – 2008. [Електронний ресурс]. – Режим доступу: https://www.kaa.org.ua/22-articles/57-дослідження-захищеності-wi-fi-мереж-в-м-києві.html

ДОДАТОК А — Модель зони покриття

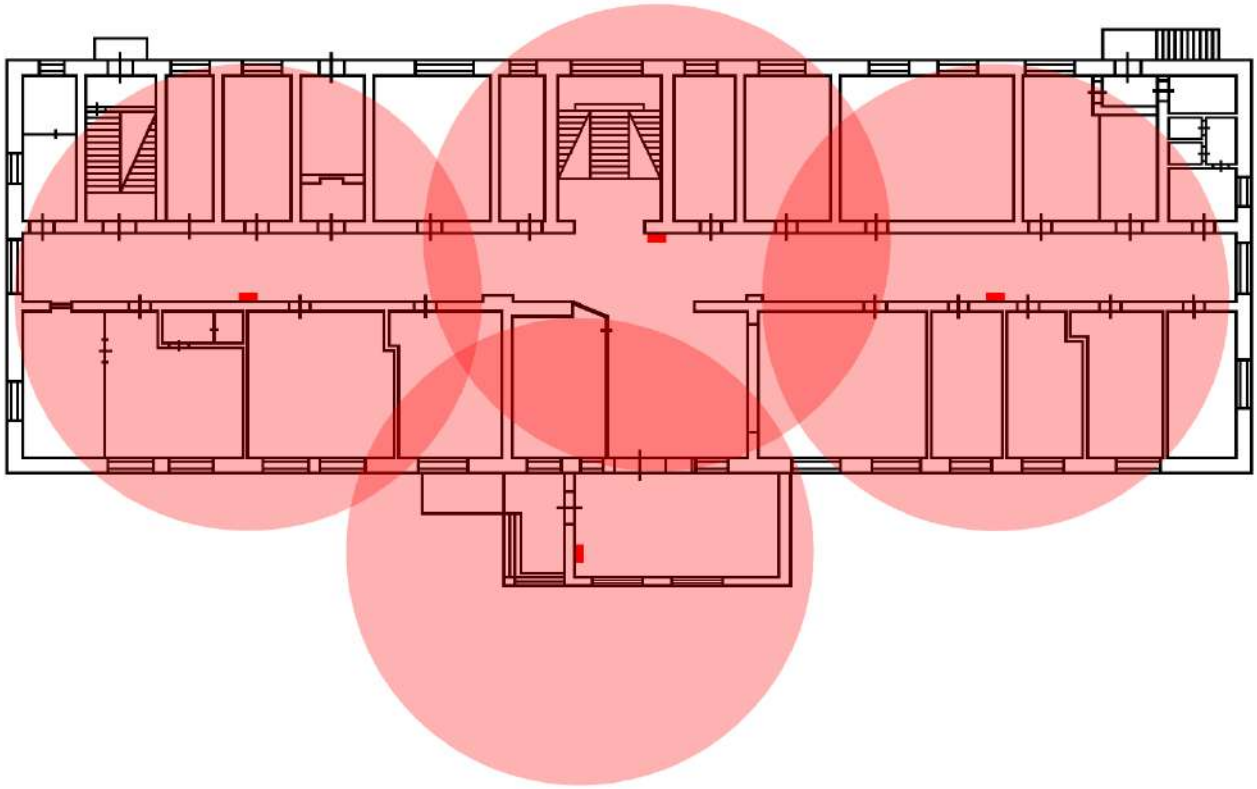


Рисунок А.1 — Модель покриття Амбулаторії №1

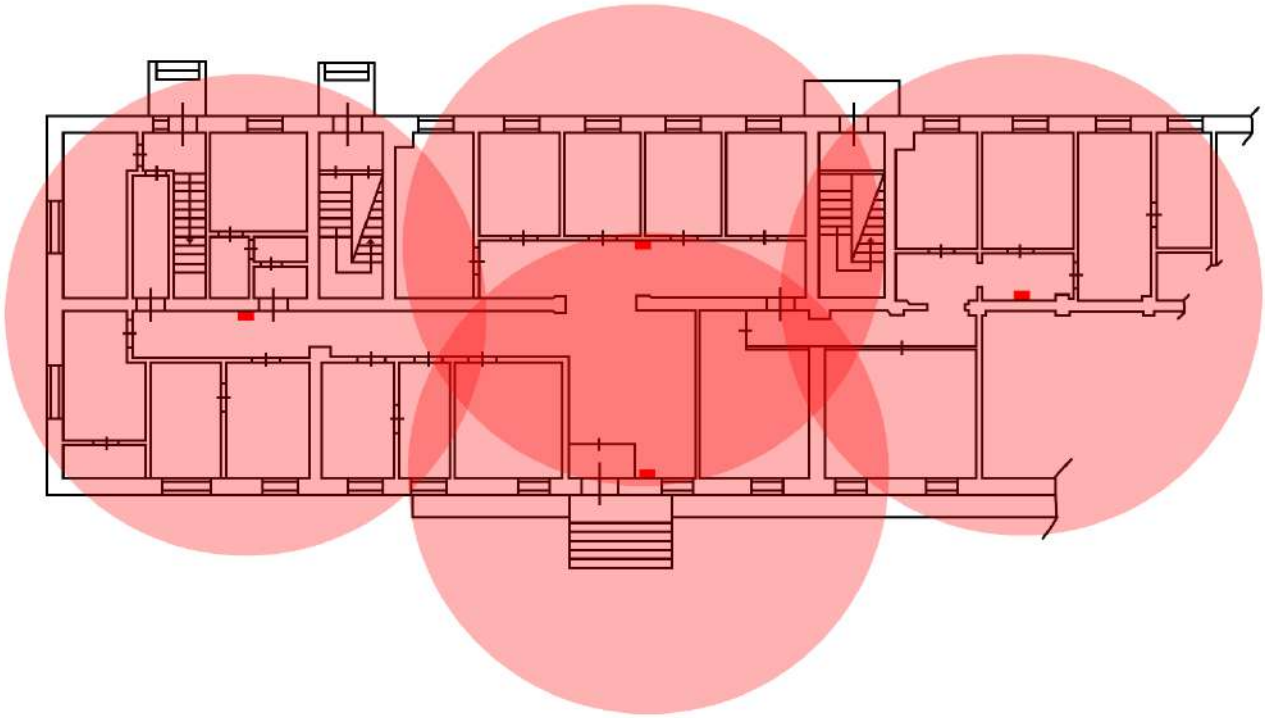


Рисунок А.2 — План Амбулаторії №2

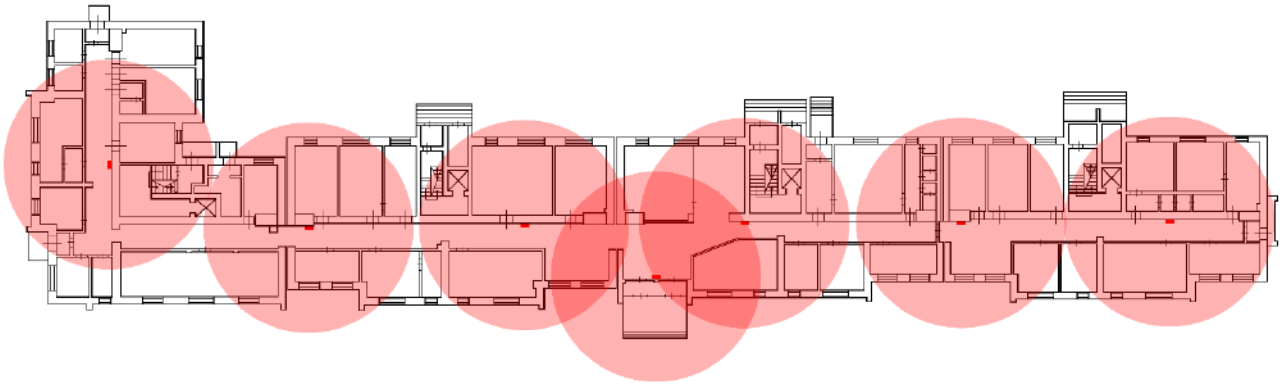


Рисунок А.3 — План Амбулаторії №3

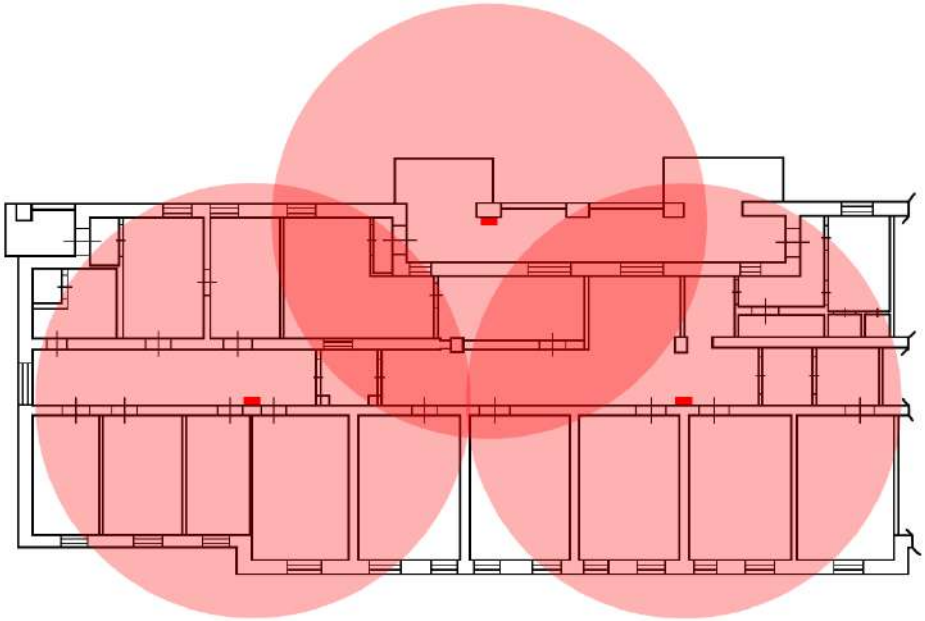


Рисунок А.4 — План Амбулаторії №4

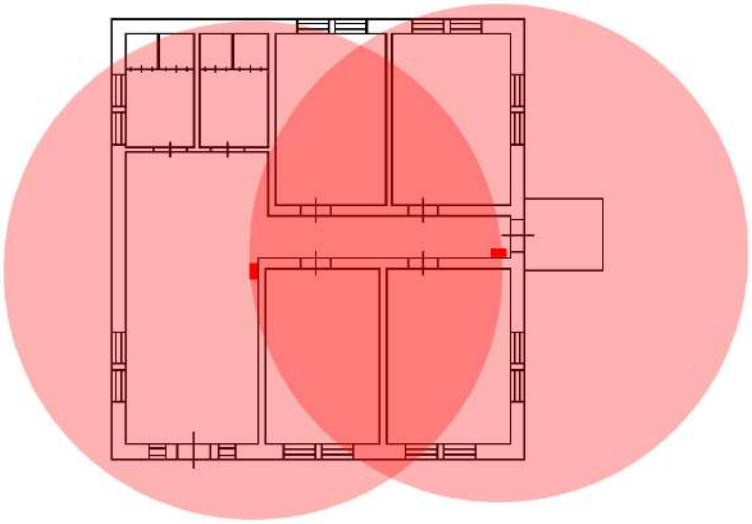


Рисунок А.5 — План Амбулаторії №5

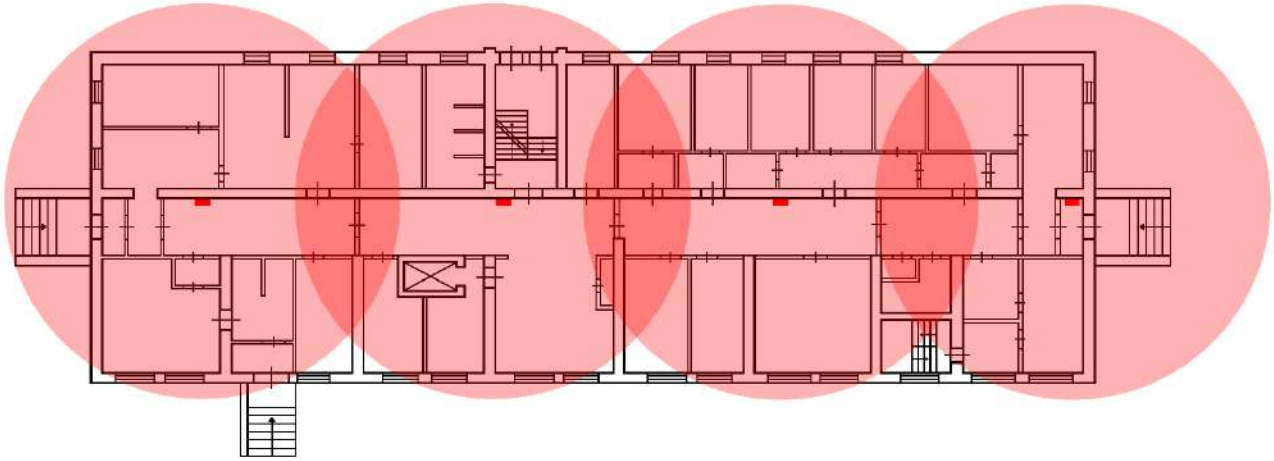


Рисунок А.6 — План Амбулаторії №6

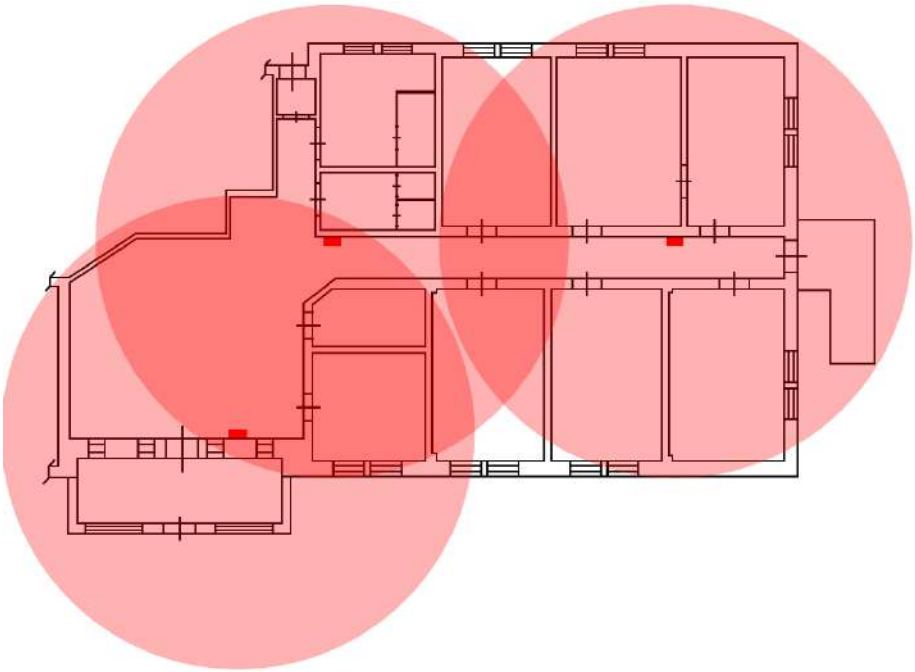


Рисунок А.7 — План Амбулаторії №10