Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки
Факультет радіоелектроніки та телекомунікацій
(повне найменування інституту, факультету)

Кафедра радіотехніки та телекомунікацій
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
бакалавра
(ступінь вищої освіти)

на тему **МОДЕРНІЗАЦІЯ МЕРЕЖІ ДОСТУПУ НАВЧАЛЬНОГО КОРПУСУ УНІВЕРСИТЕТУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ**

Виконав: студент(ка) 4 курсу, групи РТ-917

Спеціальності
172 «Телекомунікації та радіотехніка»
(код і найменування спеціальності)

Освітня програма (спеціалізація)
«Інформаційні мережі зв'язку»

Рюміна Єлизавета Володимирівна
(прізвище та ініціали)

Керівник Сметанін І.М.
(прізвище та ініціали)

Рецензент Коноваленко Ю.О.
(прізвище та ініціали)

2021 рік

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Інститут, факультет *Інститут інформатики та радіоелектроніки, ФРЕТ*
Кафедра *Радіотехніки та телекомунікацій*
Ступінь вищої освіти *Бакалавр*
Спеціальність *172 «Телекомунікації та радіотехніка»*
(код і найменування)
Освітня програма (спеціалізація) *Інформаційні мережі зв'язку*
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Завідувач кафедри *РТТ*
к.т.н., доц. *Морщавка С.В.*
«_____» *травня* 20 *21* року

З А В Д А Н Н Я
НА ДИПЛОМИНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

Рюміній Єлизаветі Володимирівні
(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) *Модернізація мережі доступу навчального корпусу університету до інформаційних ресурсів*

керівник проєкту (роботи) *Сметанін Ігор Миколайович, ст.викладач*,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від « 30 » квітня 2021 року № 164
2. Строк подання студентом проекту (роботи) *26 травня 2021 р.*
3. Вихідні дані до проєкту (роботи) *Методи доступу до інформаційних ресурсів національного університету «Запорізька політехніка» у третьому корпусі*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) *Опис задач, які повинна вирішувати проєктуєма мережа та вимоги до неї, принципи побудови бездротової мережі порівняння та вибір стандартів, розрахунок кількості користувачів та точок доступу, результати моделювання для різних сценаріїв функціонування проєктованої мережі.*
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Презентація 16 слайдів

6. Консультанти розділів проєкту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	*Сметанін І. М., ст.викладач*	02.04.21.	26.05.21
Нормокон-	*Мороз Г.В., ст. викладач*		
троль			

7. Дата видачі завдання « 2 » *квітня* 20 *21* року.

КАЛЕНДАРНИЙ ПЛАНт

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	*Пошук та вивчення наукових джерел*	*05.04-15.04*	
2	*Дослідження існуючих методів доступу до інформаційної*	*01.04-15.04*	
	мережі		
3	*Розрахунок кількості точок доступу та моделювання в програмі*	*16.04-02.05*	
	D-Link Wi-Fi Planner Pro		
4	*Моделювання в програмі OPNET*	*03.05-5.05*	
5	*Оформлення пояснювальної записки*	*5.05-15.05*	
6	*Перевірка ПЗ на доброчесність*	*18.05-19.05*	
7	*Створення презентації у Power Point*	*20.05-26.05*	
8	*Захист*	*2.06*	

Студент(ка) _____ *Рюміна Є.В.*
(підпис) (прізвище та ініціали)

Керівник бакалаврської роботи _____ *Сметанін ІМ.*
(підпис) (прізвище та ініціали)

РЕФЕРАТ

ПЗ: 70 сторінок, 19 рисунків, 9 таблиці, 15 джерел

Мета роботи – модернізація та розширення мережі третього корпусу національного університету «Запорізька політехніка».

Об’єкт дослідження – методи доступу до інформаційної мережі в третьому корпусі.

Методи дослідження – статистичні методи, методи чисельного аналізу, методи об'єктно-орієнтованого і графічного програмування.

В роботі здійснено опис та порівняння можливих послуг і додатків, які використовуються в університеті. Досліджені характеристики і вихідні дані навчального корпусу університету. Було виконано порівняння можливих технологій та вибір найбільш відповідної.

Було виконано опис існуючих стандартів, їх порівняння та вибір відповідного. Описано процес реалізації хендоверу та структурне рішення для обраного стандарту. Описано архітектура, функціональне та схемне рішення побудови проєктованої мережі з урахуванням місцевості.

Відображена методика, розрахунки максимальної кількості користувачів на одну точку доступу і мінімальна кількість точок доступу з урахуванням розташування їх на поверсі. Проведено вибір необхідного обладнання та показано процес моделювання в програмі D-Link Wi-Fi Planner Pro.

Робота в програмі OPNET. Опис етапів вибору елементів та їх налаштування, побудова моделі. Опис результатів симуляції та порівняння з розрахунковими значеннями.

БЕЗДРОТОВА МЕРЕЖА, ТОЧКА ДОСТУПУ, ІНФОРМАЦІЙНА МЕРЕЖА, WI-FI, ХЕНДОВЕР, ТЕХНОЛОГІЯ

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 7
ВСТУП 8
1 ОПИС ІСНУЮЧОЇ МЕРЕЖІ ТА ВИБІР ТЕХНОЛОГІЇ ДЛЯ ПРОЄКТОВАНОЇ 10
1.1 Опис використовуваних додатків 10
1.2 Доступ до інформаційної мережі університету 13
1.3 Характеристики третього корпусу університету 15
1.4 Вимоги до проектованої мережі 17
1.5 Порівняння та вибір технології 19
1.5.1 Технологія ZigBee (802.15.4) 19
1.5.2 Технологія Bluetooth (802.15.1) 22
1.5.3 WiMax (802.16) 24
1.5.4 Wi-Fi (802.11) 26
2 ВИБІР СТАНДАРТУ ТА ПРОЄКТУВАННЯ МЕРЕЖІ 32
2.1 Вибір стандарту технології Wi-Fi для реалізації проєкту 32
2.1.1 Стандарт IEEE 802.11i 32
2.1.2 Стандарт IEEE 802.11v 34
2.1.3 Стандарт IEEE 802.11r 35
2.2 Хендовер в бездротових мережах та стандарті 802.11r 37
2.3 Проєктування мережі 41
3 РОЗРАХУНОК КІЛЬКОСТІ ТОЧОК ДОСТУПУ ТА ВИБІР ОБЛАДНАННЯ 44
3.1 Розрахунок кількості потенційних абонентів в корпусі 44
3.2 Розрахунок кількості користувачів на одну точку доступу 47
3.3 Розрахунок кількості точок доступу 48
3.4 Моделювання в програмі D-Link Wi-Fi Planner Pro 50
3.5 Вибір обладнання 53

4 ПРОЕКТУВАННЯ МЕРЕЖІ В OPNET MODELER® 57
4.1 Опис та переваги OPNET Modeler® 57
4.2 Проектування мережы в OPNET Modeler® 59
4.3 Симуляція в пакеті OPNET Modeler® та порівняння отриманих результатів. 65
ВИСНОВКИ 68
ПЕРЕЛІК ПОСИЛАНЬ 69

ПЕРЕЛІК СКОРОЧЕНЬ

МС	–	мобільна станція
ТД	–	точка доступу
ACK	–	підтвердження
AES	–	розширений стандарт шифрування
BSS	–	набір базових послуг
DSSS	–	метод прямої послідовності для розширення спектра
EAP	–	розширюваний протокол автентифікації
FHSS	–	розширення спектра при стрибкоподібній зміні частоти
LAN	–	локальна мережа
PMK	–	парний майстер-ключ
QoS	–	якість обслуговування
TKIP	–	протокол цілісності тимчасового ключа
WLAN	–	бездротова локальна мережа

ВСТУП

Використання систем бездротових локальних мереж (WLAN) швидко зростає в комунікаційної індустрії. WLAN можуть використовуватися або для заміни провідних локальних мереж, або в якості розширення інфраструктури провідних локальних мереж.

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

Бездротові мережі мають, в порівнянні з традиційними провідними мережами, чималі перевагами, головним з яких є:

а) простота розгортання;

б) гнучкість архітектури мережі, коли забезпечується можливість динамічної зміни топології мережі при підключенні, пересуванні і відключенні мобільних користувачів без значних втрат часу;

в) швидка інсталяція. Для початку роботи з бездротовою мережею немає необхідності проводити монтажні роботи. Досить налаштувати точку доступу та підключити її до існуючої мережі;

г) висока мобільність.

Оскільки ріст сучасних технологій невпинно зростає тоді і потреба у використанні сучасних методів навчання також. Тоді постає необхідність забезпечення навчального закладу доступом до сучасних технологій. Виходячи із цього дана робота присвячена модернізації бездротової мережі в університеті. Метою проектування є не тільки розширення мережі та забезпечення надійним радіопокриттям, але і надання можливості

користувачеві вільного переміщення між точками доступу. Зручність полягає в тому, що сеанс зв'язку або обмін даними не буде перериватись при переході від однієї точки доступу до іншої.

1 ОПИС ІСНУЮЧОЇ МЕРЕЖІ ТА ВИБІР ТЕХНОЛОГІЇ ДЛЯ ПРОЄКТОВАНОЇ

1.1 Опис використовуваних додатків

В сучасних умовах якісна організація навчального і наукового процесів, ефективність управлінської діяльності нерозривно пов'язані з впровадженням та використанням сучасних інформаційних технологій і телекомунікацій.

Для побудови мережі на основі технології бездротової та дротової передачі даних необхідно зрозуміти які послуги найбільше використовують, які додатки надають ці послуги та який об'єм споживаного трафіку. Зазвичай під час навчання та науково-дослідницької діяльності використовуються пошукові системи та веб-сторінки, які надають доступ до необхідної інформації. Але під час дистанційної та змішаної форми навчання, велика увага приділяється додаткам, які здатні надати послуги аудіо- та відеозв’язку, on-line конференції на велику кількість користувачів.

Нижче наведено найпопулярніші додатки, їх характеристика та споживаний трафік. Найбільш використовуваними додатками на території університету є: освітня платформа Moodle; відеохостинг YouTube; месенджери Telegram, Viber, WhatsApp; Zoom; пошукова система Google.

Освітня *платформа Moodle* – система управління курсами (електронне навчання), також відома як система управління навчанням або віртуальне навчальне середовище є абревіатурою від англ. Modular Object-Oriented Dynamic Learning Environment (модульне об'єктно-орієнтоване динамічне навчальне середовище).

Підтримувані формати: текст, зображення, відео, SCORM 2004, 1.2; IMS; LTI 1.1, 1.3, 2.0 [1].

Використовуваний трафік – 2-5 Мб/год.

YouTube – відеохостинг, що надає послуги розміщення відеоматеріалів. В процесі навчання використовується для знаходження додаткової та нової інформації.

Підтримувані формати: відео.

Використовуваний трафік – 300 Мб/год-1,5 Гб/год.

Telegram – багатоплатформовий месенджер з функціями VoIP, що дозволяє обмінюватися текстовими, голосовими та відеоповідомленнями, стікерами та фотографіями, файлами багатьох форматів. Також можна здійснювати відео- і аудіодзвінки, організовувати конференції, розраховані на багато користувачів групи і канали.

Використовуваний трафік – 0,42 Мб/год – 3,75 Мб/год (включаючи відео- і аудіозв’язок).

Viber – застосунок VoIP телефонія та обмін текстовими повідомленнями. Інтегрується з адресною книгою та авторизується за номером телефону. Дозволяє здійснювати безкоштовні дзвінки (оплата тільки за інтернет-трафік), а також передавати текстові повідомлення, зображення, відео- та аудіо- повідомлення.

Використовуваний трафік – 14 Мб/год (включаючи відео- і аудіозв’язок).

WhatsApp – популярна безкоштовна система миттєвого обміну текстовими повідомленнями для мобільних і інших платформ з підтримкою голосового зв'язку і відеозв'язку. Дозволяє пересилати текстові повідомлення, зображення, відео, аудіо, електронні документи та навіть програмні установки через Інтернет.

Використовуваний трафік – на відправку одного повідомлення, довжиною в 500 символів витрачається приблизно 800 байт. Найбільше трафіку споживається при розмові – приблизно від 700 Кбайт до 1 Мб за одну хвилину розмови [2].

Zoom – хмарна платформа для організації відеоконференцій, розроблена компанією Zoom Video Communications. Вона надає сервіс відеотелефонії, який дозволяє підключати одночасно до 100 пристроїв безкоштовно, з 40-хвилинним обмеженням для безкоштовних акаунтів.

Використовуваний трафік – 540 Мб/год-1,62 Гб/год (при спілкуванні «один на один»), 810 Мб/год-2,4 Гб/год (відеоконференція з трьома і більше учасниками) [3].

Пошукова система Google – алгоритм та сукупність комп'ютерних програм, що надає користувачеві можливість швидкого доступу до необхідної йому інформації. Одне з найбільших відомих застосувань – веб-сервіси для пошуку текстової або графічної інформації.

Використовуваний трафік – 1,5 Мб/год-12 Мб/год.

Порівняння використовуваного трафіку різними додатками зображено на рисунку 1.1.

Рисунок 1.1 – Порівняння використовуваного трафіку різними додатками

Враховуючи таке різноманіття необхідних платформ і додатків для дистанційної та змішаної форми навчання потрібна розвинена мережа доступу до інформації в університеті та Інтернет.

1.2 Доступ до інформаційної мережі університету

Як згадувалося вище важливе значення має наявність розвиненої мережі, що забезпечує надійну, високошвидкісну взаємодію між навчальними, науковими і адміністративним нормативними підрозділами, а також доступ до власних інформаційних ресурсів, ресурсів науково-освітніх мереж і мережі Інтернет.

Основу інформаційної мережі складає кабельні лінії зв'язку, які заведені до кожного учбового корпусу університету. В університеті функціонує 46 комп'ютерних класів, кожен з яких об'єднаний у власну локальну мережу. За допомогою локальної мережі є можливим організовувати обмін файлами, спільно використовувати обчислювальні і апаратні ресурси, поєднувати розподілену обробку даних на декількох комп'ютерах з централізованим зберіганням інформації. 1528 комп'ютерів мають вихід до мережі Інтернет.

Окрім комп'ютерних класів, використання інформаційної мережі університету можливо в бібліотеці, де є доступ не тільки до власних інформаційних ресурсів, а і до мережі Інтернет. Такими інформаційними ресурсами є: електронний каталог, електронна бібліотека, доступ до світової наукової інформації.

Останнім часом для більш ефективної наукової роботи та ведення адміністративної діяльності на кафедрах створюються власні кафедральні мережі, які також під'єднані до загальної мережі університету. З розвитком переносних приладів обміну інформацією такі мережі потребують окрім використання кабельних ліній зв'язку, ще залучення технологій бездротового

зв’язку. Враховуючи вартість і простоту доступу до інформаційної мережі найбільш оптимальним було б використання бездротового зв’язку на основі технології Wi-Fi. За допомогою цієї технології є можливість доступу до власних інформаційних ресурсів та виходу до глобальної мережі Інтернет (рис.1.2). Зараз точки доступу Wi-Fi встановлені переважно на кафедрах університету, тому використання цієї технології доступу до інформаційної мережі є обмеженим. Тому гостро виникає питання щодо модернізації існуючої мережі до сучасних вимог.

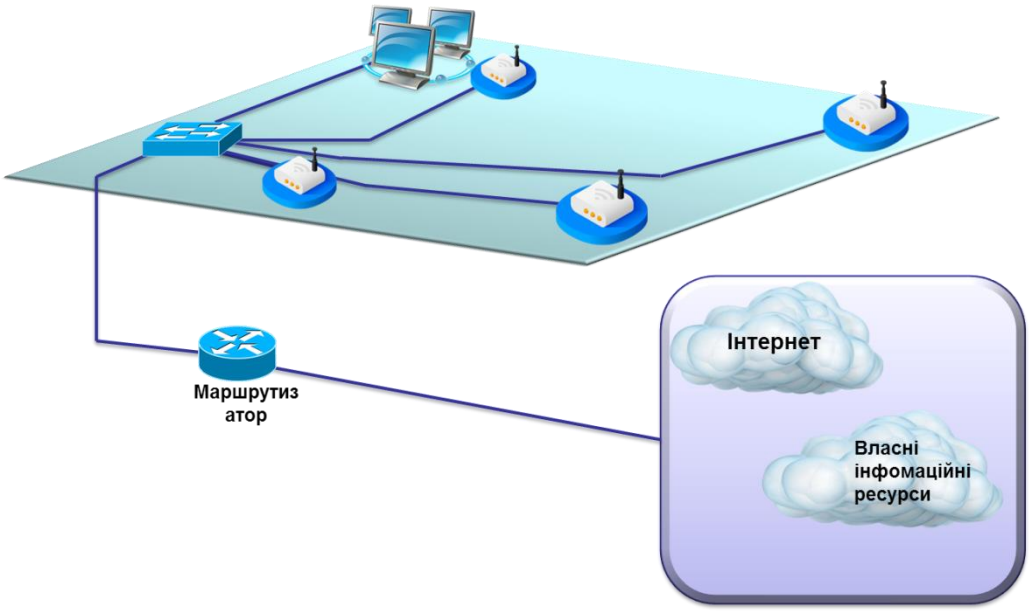

Рисунок 1.2 – Існуючий доступ до інформаційної мережі

Запропонованим варіантом вирішення проблеми обмеженості доступу до інформаційної мережі є розширення та модернізація існуючої бездротової мережі (рис.1.3). Під розширенням розуміється додавання до вже існуючих точок доступу нових, для того, щоб забезпечити всю площу третього корпусу радіо покриттям. Завдяки розширенню доступ до інформаційних ресурсів буде можливий в більшій частині будівлі. Під модернізацією розуміється забезпечення можливістю вільного пересування між точками доступу без

перереєстрації в новій. Реєстрація здійснюється лише при підключенні до початкової точки доступу.

Завдяки бездротовій мережі буде можливим доступ до інформаційних ресурсів в будь-якій точці університету. Створення такої мережі призведе до полегшення навчального процесу, шляхом використання мобільних пристроїв, які не прив’язані до конкретних аудиторій.

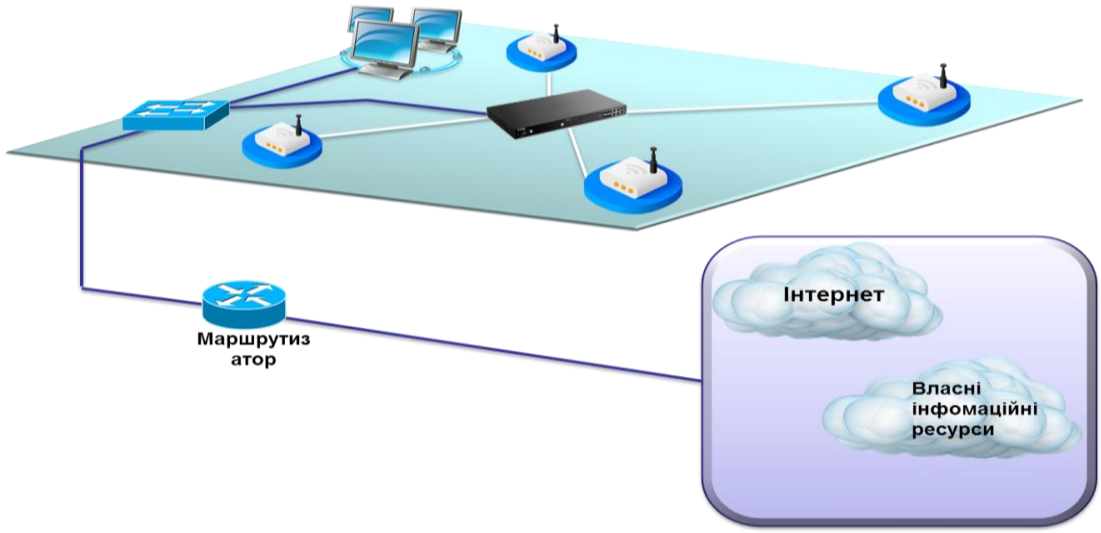

Рисунок 1.3 – Запропонований варіант доступу до інформаційної мережі

Модернізацію існуючої мережі треба виконувати поетапно в кожному навчальному корпусі. Одним з корпусів університету, де велика кількість аудиторій і висока щільність студентів та викладачів є третій корпус. Тому в даній роботі розглядається можливість модернізації існуючої мережі саме цього корпусу.

1.3 Характеристики третього корпусу університету

Третій корпус знаходиться у внутрішньому дворі Національного університету «Запорізька політехніка». Корпус є відокремленою спорудою від інших корпусів. Споруда складається з п’яти поверхів. Площа першого поверху становить 863 м^2. Площа другого поверху – 769 м^2. Площа третього, четвертого та п’ятого поверхів складає 743 м^2. Кожен поверх має навчальні аудиторії. На першому поверсі знаходиться чотири навчальні аудиторії та бібліотека. Загальна площа навчальних аудиторій першого поверху складає 346,25 м^2. Другий поверх складається з восьми аудиторій, загальна площа аудиторій – 373,75 м^2. Третій поверх має вісім предметних аудиторій, загальною площею 522 м^2. Четвертий складається з семи аудиторій, із загальною площею 447 м^2. П’ятий поверх – сім предметних аудиторій, загальна площа – 498 м^2. В загальному підрахунку площа навчальних аудиторій, складає 2187 м^2.

До учбового корпусу прокладено кабельні лінії зв’язку. В корпусі знаходяться комп’ютерні класи. В комп’ютерних класах пристрої об’єднані в локальну мережу за допомогою технології Ethernet. Кожен комп’ютер підключений до виходу в глобальну мережу Інтернет.

Зараз в корпусі використовується не лише кабельні мережі, але і бездротові, на основі технології Wi-Fi (рис.1.4). При цьому точки доступу, що розташовані на кафедрах, які знаходяться в третьому корпусі не об’єднані в єдину систему доступу і не забезпечують можливість одноразової реєстрації та вимагають подальших перереєстрацій на кожній. Також їх розташування на поверхах корпусу не надають повного та якісного покриття задля отримання абонентами бездротового доступу. На прикладі третього поверху корпусу видно, що у кожної з розташованих там кафедр та й аудиторіях існують свої окремі мережі.

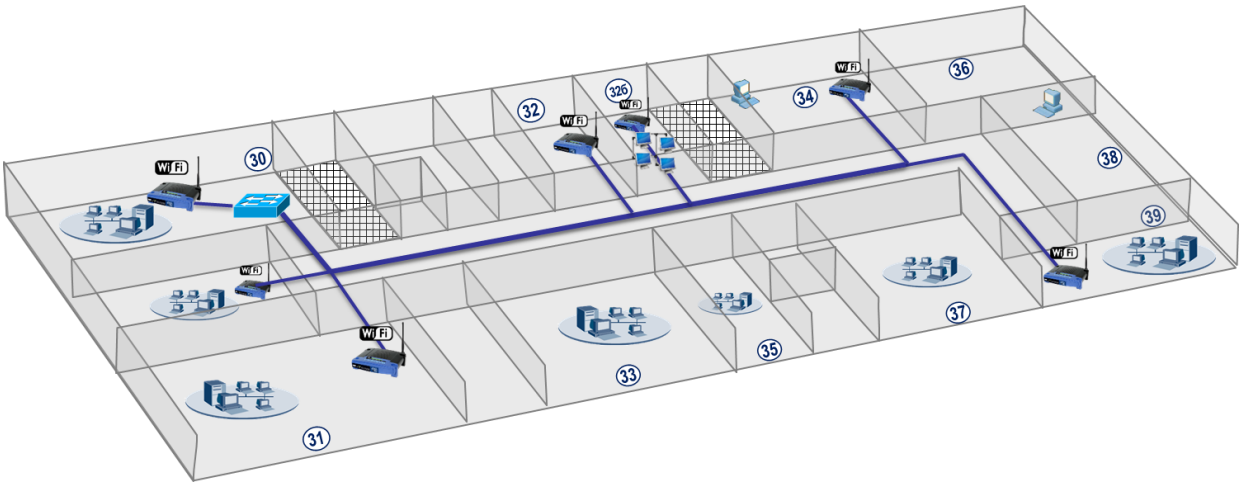

Рисунок 1.4 – Існуюче розміщення комутаційного обладнання та підмереж

Отже, звертаючи увагу на те, що все ж мережа існує і потребує модернізації, а також є певний запит на роботу з бездротовими приладами, то перш ніж приступити до проектування виникає необхідність в чіткому визначенні вимог щодо нової мережі.

1.4 Вимоги до проектованої мережі

Як вже зрозуміло з попередніх міркувань, головною метою є модернізація існуючої мережі, задля охоплення усіх п’яти поверхів безперервним бездротовим покриттям, можливістю одноразової реєстрації і без подальших перереєстрацій на кожній ТД. При цьому треба враховувати, що покриття повинно бути повним та якісним не тільки в коридорах корпусу, але й в навчальних аудиторіях.

Враховуючи, те що в пункті 1.1 були описані усі додатки, які використовуються в університеті, то необхідно щоб мережа забезпечувала підтримку всіх форматів, які використовуються в додатках. Різні формати даних, які передаються, використовують різний об'єм трафіку від 0,42 Мб/год до 2,4 Гб/год, тому дуже важливо, щоб пропускна здатність відповідала використовуваному трафіку. Не менш важливою вимогою є передача

великого об'єму даних та мінімізація втрати будь-яких даних. Необхідно зауважити, що під час модернізації мережі враховувалась можливість використання голосу та відеозв’язку. Без QoS можуть виникнути такі проблеми з якістю: тремтіння, втрата пакетів та великий час кругового шляху (RTT). Тому необхідно врахувати, що застосування QoS є необхіднім при використанні голосового та відеозв’язку для забезпечення відповідної якості.

Також, на сьогоднішній день інформація та володіння нею відіграє важливу роль у житті, тому безпека – є важливим критерієм при проєктуванні мережі. З огляду на те, що мережа проектується на основі бездротових технологій важливим є електромагнітна сумісність та забезпечення відповідних санітарно-гігієнічних норм мережі. Останньою вимогою є відносно невелика ціна. Важливим критерієм для скорочення витрат є використання не ліцензованої смуги частот. Для того щоб в подальшому використанні мережа не вимагала великих витрат, електроспоживання має бути відносно невеликим.

Таким чином, можна скласти основні вимоги до проектованої мережі:

– забезпечення надійним радіо покриттям всієї необхідної території;

– мережа повинна підтримувати хендовер;

– підтримка передачі даних форматів: текстові повідомлення та файли, графічне повідомлення, потокові аудіо- і відео повідомлення, відеозв’язок, і т.і.;

– забезпечення необхідною пропускною здатністю, що надавала б можливість використання різних додатків з VoIP-телефонії та відеозв’язку, які дуже вимогливі до QoS мережі;

– забезпечення низькою ймовірність втрати даних.

– у разі потреби, можливість обміну достатньо великими об’ємами інформації;

– безпека бездротової мережі. Це завдання включає такі аспекти, як автентифікація користувачів , їх авторизація, захист даних, що передаються;

– забезпечення необхідного рівня електромагнітної сумісності роботи ТД проміж собою та іншими системами;

– забезпечення виконання необхідного рівня санітарно-гігієнічних вимог до мереж радіозв’язку;

– відносно невелика ціна на модернізацію мережі та відсутність ліцензування;

– відносно невелике електроспоживання.

Розглянувши і склавши основні вимоги до проектованої мережі виникає необхідність в виборі технології, яка найбільш оптимально буде відповідати цім вимогам для бездротової передачі даних в існуючих умовах.

1.5 Порівняння та вибір технології

Для того, щоб вибрати найбільш відповідну технологію бездротової передачі даних, нижче приведено опис та порівняльна таблиця бездротових технологій. В попередньому пункті були приведені критерії, яким має відповідати вибрана технологія. Згідно цих критеріїв до розгляду було взято чотири технології, які найбільш підходять до виконання поставлених завдань, а саме: ZigBee (802.15.4), Bluetooth (802.15.1), WiMax (802.16), Wi-Fi (802.11).

Як можна побачити, ці технології належать до однієї групи стандарту IEEE, IEEE 802. IEEE 802 – група, яка охоплює локальні мережі (LAN) та мережі мегаполісів (MAN). Служби та протоколи цього стандарту знаходяться на двох нижніх рівнях фізичному та канальному. Це пов’язано з тим, що саме ці два рівня в найбільшій мірі відображають специфіку локальних мереж. Тому, в описі технологій буде приведено характеристика цих двох рівнів.

1.5.1 Технологія ZigBee (802.15.4)

Зв'язок Zigbee спеціально побудований для контрольних та сенсорних мереж за стандартом IEEE 802.15.4 для бездротових персональних мереж (WPAN), широко розповсюджений для управління та моніторингу. Цей стандарт зв'язку визначає фізичний та канальний рівні для обробки багатьох пристроїв, але з низькою швидкістю передачі даних. Ця система зв'язку є менш дорогою та простішою, ніж інші фірмові мережі бездротових технологій короткого діапазону, такі як Bluetooth та Wi-Fi.

Структура системи Zigbee складається з трьох різних типів пристроїв, таких як Zigbee координатор, маршрутизатор і кінцевий пристрій. Кожна мережа Zigbee повинна складатися як мінімум з одного координатора, який виступає в якості кореня і моста мережі. Координатор відповідає за обробку та зберігання інформації під час виконання операцій з прийому та передачі даних.

Маршрутизатор Zigbee виступають в якості проміжних пристроїв, які дозволяють передавати дані на інші пристрої. Кінцеві пристрої мають обмежену функціональність для зв'язку з батьківськими вузлами, що дозволяє економити заряд батареї. Кількість маршрутизаторів, координаторів і кінцевих пристроїв залежить від типу мережі.

Архітектура протоколу Zigbee складається з стека різних рівнів, де IEEE 802.15.4 визначає фізичний і канальний рівень. Канальний рівень складається з підрівні MAC (стандарт IEEE 802.15.4) і підрівнів управління логічним каналом LLC (стандарт IEEE 802.2). Підрівень SSCS описує взаємодію зі специфічною службою MAC [4].

Фізичний рівень. Цей рівень виконує операції модуляції та демодуляції під час передачі та прийому сигналів відповідно.

Підрівень MAC 802.15.4 надає дві служби для вищих рівнів OSI, до яких може бути здійснений доступу через дві точки доступу до служб (SAP).

Служба передачі даних рівня MAC включається через загальну частину MAC-підрівня (MCPS-SAP), служба управління рівня MAC – через

MAC-рівень управління станом (MLME-SAP). Ці дві служби забезпечують інтерфейс між SSCS (або LLC) і фізичним рівнем [5].

Побудовані за цим стандартом WPAN мережі працюють на частотах 868 МГц, 902-928 МГц і 2,4 ГГц. Швидкість передачі даних 250 кбіт/с. Радіус дії 10-100 метрів.

Безпека. Цей стандарт використовує алгоритм шифрування AES-128 і модифікований алгоритм CCM для управління ключами і блоками. Такий механізм шифрування працює відразу на двох рівнях стека протоколу – мережевому рівні (NWK) і рівні додатку (APL). З урахуванням того, що специфікація ZigBee допускає різну топологію мереж, то і модель системи безпеки (security model), яка використовується в мережі, теж може бути різною – централізованої або розподіленої. Основна модель – централізована. Вона передбачає призначення спеціального довіреного центру управління ключом (ZigBee Trust Center). Розподілена модель передбачає, що пристрої в мережі при встановленні зв'язку та обміні даними використовують власні ключі і не звертаються ні до якого централізованого сервісу [6].

Переваги ZigBee:

– відносна дешевизна;

– використання не ліцензованої смуги частот;

– невелике споживання енергії;

– ця мережа має гнучку мережеву структуру;

– налаштування мережі дуже просте;

– навантаження рівномірно розподілені по мережі, тому що в ній немає центрального контролера;

– мережа є масштабованої і легко додавати / видаляти кінцеве пристрій.

Але відповідно до вимог проектованої мережі цьому стандарту притаманні достатньо важливі недоліки, а саме:

– швидкість передачі Zigbee менша, у порівнянні з Wi-Fi;

– слабка захищеність системи;

– у порівнянні з Wi-Fi, він є менш безпечним;

– висока вартість заміни, як тільки виникає проблема з пристроями на базі Zigbee.

1.5.2 Технологія Bluetooth (802.15.1)

Bluetooth – це низькорівневий, спеціальний, наземний, бездротовий стандарт для ближнього зв'язку. Він призначений для невеликих і недорогих пристроїв з низьким енергоспоживанням. Технологія працює з трьома різними класами пристрою: клас 1, клас 2 і клас 3, де дальність дії близько 100 метрів, 10 метрів і 1 метр відповідно [7].

Технологія Bluetooth передбачає два види зв'язку: синхронну – SCO (Synchronous Connection Oriented) і асинхронну – ACL (Asynchronous Connectionless). Перший вид, SCO, розрахований на встановлення симетричного з'єднання "точка-точка" і служить переважно для передачі мовних повідомлень. Швидкість передачі інформації SCO дорівнює 64 Кіт/с. Другий, ACL, призначений для пакетної передачі даних. Він підтримує симетричні і асиметричні з'єднання типу "точка-багато точок". Швидкість передачі пакетної інформації при ACL складає близько 721 Кбіт/с. Пакети даних мають фіксований формат.

Основоположним принципом побудови систем Bluetooth є використання методу розширення спектра при стрибкоподібній зміні частоти (FHSS – Frequency Hop Spread Spectrum). Виділений для Bluetooth-радіозв'язку частотний діапазон дорівнює 2,402-2,480 ГГц. Смуга кожного каналу 1 МГц, рознос каналів – 140-175 кГц. Для кодування пакетної інформації використовується частотна маніпуляція.

Зміна каналів проводиться по псевдовипадковому закону 1600 разів в секунду. Постійне чергування частот дозволяє радіоінтерфейсу Bluetooth

транслювати інформацію по всьому діапазону і уникнути впливу перешкод з боку пристроїв, що працюють в цьому ж діапазоні. Якщо даний канал зашумлений, то система перейде на інший, і так буде відбуватися до тих пір, поки не виявиться канал, вільний від перешкод.

Архітектура Bluetooth. Блок Radio займається перетворенням бітової послідовності в радіо сигнали. Питанням модуляції, спектральних характеристик і фізики процесів забезпечення бітової швидкості – все це вирішується на нижньому рівні моделі.

Baseband Layer = Link Controller + Baseband Manager + Device Manager

Рівень baseband представлений у вигляді трьох блоків, спільна задача яких полягає в управлінні фізичними каналами, поверх яких встановлюються фізичні з'єднання. Bluetooth-адресація, синхронізації генераторів пристроїв, управління кодами доступу до фізичних каналах, пошук пристроїв і встановлення фізичного каналу між ними – все це завдання Baseband-рівня.

Link Manager. Після того, як два нижніх рівні забезпечили фізичним з'єднанням між пристроями, справа стає за організацією логічних каналів, які згодом і стануть базою для передачі трафіку додатків. Link Managerв відповідає за встановлення, зміну і звільнення логічних з'єднань між пристроями, а так само за оновлення параметрів фізичних з'єднань. Для цих цілей Link Manager використовує Link Management протокол (LMP).

L2CAP Layer = Channel Manager + L2CAP Resource Manager

Logical Link Control and Adaptation Protocol (L2CAP) – протокол, який працює поверх створених логічних з'єднань, що забезпечує сегментацію і відновлення пакетних даних від всіх вище додатків [8].

Безпека. Bluetooth пропонує безпеку користувача і конфіденційність інформації. А саме, він використовує 128-бітове випадкове число, 48-бітну MAC-адресу пристрою і два ключа: авентифікації (128 біт) і шифрування (від 8 до 128 біт). Безпека має 3 рівня: незахищений, рівень обслуговування і підключення.

Переваги Bluetooth:

– відносно велика дальність дії;
– Bluetooth використовується для передачі голосу і даних;
– використання не ліцензованої смуги частот;
– має низьке енергоспоживання;
– дозволяє уникнути перешкод від інших бездротових пристроїв;
– пристрої Bluetooth доступні за дуже низькою ціною;
– легко оновлюється.

Але відповідно до вимог проектованої мережі цьому стандарту притаманні достатньо важливі недоліки, а саме:

– низька пропускна здатність у порівнянні з Wi-Fi;
– при певних умовах він може втратити зв'язок;
– менш безпечний у порівнянні з Wi-Fi.

1.5.3 WiMax (802.16)

WiMax – це стандарт бездротового зв'язку, що забезпечує широкосмуговий зв'язок на значні відстані зі швидкістю, порівняною з кабельними з'єднаннями. У стандарті 802.16 передбачені діапазони 2 ... 11 ГГц і 10... 66 ГГц. У діапазоні частот 10... 66 ГГц радіоз’язок можливий лише у випадку прямої видимості між точками. В діапазоні 2...11 ГГц підтримуються три специфікації радіоінтерфейсу, що допускають можливість вирішення завдань радіозв'язку в умовах багатопроменевого поширення і

відсутністю прямої видимості (NLOS). Мережі WiMAX мають діапазон ширини смуги частот від 1,25 МГц до 20 МГц [5].

Архітектура WiMax. Два основних рівня – це MAC та фізичний рівні. MAC-рівень включає у себе три підрівні: підрівень безпеки, загальний підрівень MAC-протоколу 802.16, підрівень узгодження з протоколами послуг.

Фізичний рівень – визначає вид використовуваних для передачі даних сигналів, способи маніпуляції та завадостійкого кодування, алгоритм формування логічних каналів.

Підрівень безпеки – відбувається шифрування даних для забезпечення конфіденційності роботи користувача.

Загальний підрівень – виконує основну функцію по плануванню, обробці і виділенню ресурсів, встановлення і підтримання з'єднань, підтримка QoS.

Підрівень узгодження – погоджує формати даних протоколів вищих рівнів і даних MAC-підрівня 802.16. Дані перетворюються в пакети MAC SDU(service data unit), при цьому формується ідентифікатор з'єднань, протоколів [9].

Безпека.

WiMAX використовує протоколи безпеки, такі як протокол управління ключами секретності 2 (PKMP2), протокол розширюваної автентифікації (EAP) та стандарт розширеного шифрування (EAS). Ці протоколи забезпечують захист якості обслуговування (QoS) як аудіо-, так і відеопотоків.

Переваги WiMax:

– великий радіус дії;

– підтримка високошвидкісної передачі голосу і даних на великі відстані;

– висока пропускна здатність;

– підтримка якості обслуговування QoS;

– високий рівень безпеки;

– одна станція може обслуговувати сотні користувачів одночасно.

Але відповідно до вимог проектованої мережі цьому стандарту притаманні достатньо важливі недоліки, а саме:

– велике енергоспоживання;

– велика споживча потужність;

– вимагає великих витрат;

– складність монтажних робіт;

– велика вартість установки та експлуатації.

1.5.4 Wi-Fi (802.11)

Торгова марка Wi-Fi Alliance та загальновживана назва для стандарту IEEE 802.11 передачі цифрових потоків даних по радіоканалах.

Стандарт 802.11 визначає два типи обладнання – точка доступу (ТД) і клієнт. Точка доступу виконує роль моста між бездротовими і дротовими мережами, та зазвичай містить в собі приймач, інтерфейс дротової мережі (802.3), а також програмне забезпечення, що займається обробкою даних. Клієнтом зазвичай є комп'ютер, який укомплектований бездротовою мережевою інтерфейсною картою (Network Interface Card, NIC).

Стандарт IEEE 802.11 визначає два режими роботи мережі – режим "Ad-hoc" і клієнт/сервер (або режим інфраструктури – infrastructure mode).

Архітектура 802.11 має два рівні: фізичний та канальний.

Фізичний рівень. На фізичному рівні визначені два широкосмугових радіочастотних метода передачі та один – в інфрачервоному діапазоні. Радіочастотні методи працюють в не ліцензованому діапазоні 2,4 ГГц і 5 ГГц. Технології широкосмугового сигналу, що використовуються в радіочастотних методах, збільшують надійність, пропускну здатність, дозволяють багатьом

непов'язаним один з одним пристроям розділяти одну смугу частот з мінімальними перешкодами один для одного.

Стандарт 802.11 використовує метод прямої послідовності (Direct Sequence Spread Spectrum, DSSS) для навмисного розширення спектра сигналів, які передаються і метод частотних стрибків (Frequency Hopping Spread Spectrum, FHSS), цей метод застосовний тільки якщо пропускна спроможність не перевищує 2 Мбіт/с, так що в доповненні IEEE 802.11b залишився лише DSSS.

Канальний рівень 802.11 складається з двох підрівнів: управління логічним зв'язком (Logical Link Control, LLC) і управління доступом до носія (Media Access Control, MAC). 802.11 використовує той же LLC і 48-бітову адресацію, що і інші мережі 802, що дозволяє легко об'єднувати бездротові і дротяні мережі, однак MAC рівень має кардинальні відмінності. 802.11 використовує модифікований протокол, відомий як Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), або Distributed Coordination Function (DCF). CSMA/CA намагається уникнути колізій шляхом використання явного підтвердження пакета (ACK), що означає, що приймаюча станція посилає ACK пакет для підтвердження того, що пакет отриманий неушкодженим. MAC рівень 802.11 надає можливість розрахунку CRC і фрагментації пакетів. Кожен пакет має свою контрольну суму CRC, яка розраховується і прикріплюється до пакету. Фрагментація пакетів дозволяє розбивати великі пакети на більш маленькі при передачі по радіоканалу, що корисно в дуже "заселених" середовищах або в тих випадках, коли існують значні перешкоди, так як у менших пакетів менші шанси бути пошкодженими. Цей метод в більшості випадків зменшує необхідність повторної передачі і, таким чином, збільшує продуктивність всієї бездротової мережі. MAC рівень відповідальний за збір отриманих фрагментів, роблячи цей процес "прозорим" для протоколів більш високого рівня.

Безпека. Стандарт 802.11 спочатку передбачав апаратний протокол шифрування даних WEP (Wired Equivalent Privacy), що базується на алгоритмі шифрування RC4. Але незабаром було знайдено його уразливості, тому зараз ця технологія вже не застосовується.

WEP змінила нова технологія WPA (Wi-Fi Protected Access). Головна особливість нової системи безпеки полягає в шифруванні даних з динамічно змінюваними ключами і перевіркою автентифікації користувачів.

На відміну від WEP тут застосовується протокол цілісності тимчасових ключів TKIP (Temporal Key Integrity Protocol), що має на увазі оновлення ключів перед початком кожної сесії шифрування і перевіркою пакетів на приналежність до даної сесії.

Існує два режими автентифікації: Enterprise – перевірка здійснюється серверами RADIUS; Pre-Shared Key (WPA-PSK) – кожен вузол вводить пароль для доступу до мережі.

WPA2 (Wireless Protected Access ver. 2.0) – це друга версія набору алгоритмів і протоколів, які забезпечують захист даних в бездротових мережах Wi-Fi. З 2006 року WPA2 повинна підтримувати все вироблене Wi-Fi обладнання. Новий стандарт передбачає, зокрема, обов'язкове використання більш потужного алгоритму шифрування AES (Advanced Encryption Standard) і автентифікації 802.1X. Як і в WPA є два режими роботи: Pre-Shared Key і Enterprise.

Переваги Wi-Fi:

– достатньо великий радіус дії;

– висока пропускна здатність;

– висока швидкість передачі даних;

– безпека;

– недороге розгортання - для встановлення не потрібно багато витрат на інфраструктуру;

– використання не ліцензованої смуги частот;

– доступ до мережі відбувається миттєво завдяки простому та швидкому встановленню;

– мобільність;

– мережею можуть одночасно користуватися кілька пристроїв.

Недоліки:

– відносно велике енергоспоживання;

– перешкоди: існування електромагнітних хвиль в приміщенні може перешкоджати сигналу з'єднання.

Таким чином розглянувши всі чотири технології, які найбільш підходять до виконання поставлених завдань згідно визначених критеріїв, можна скласти таблицю їх порівнянь (табл. 1.1).

Таблиця 1.1 – Порівняння технологій

	ZigBee	Bluetooth	WiMax	Wi-Fi
Смуга частот	868/915МГц, 2,4ГГЦ	2,4 ГГц	2 ... 11 ГГц і 10... 66 ГГц	2,4 ГГц, 5ГГц
Швидкість передачі даних	250 кбіт/с	1 Мбіт/с	70 Мбіт/с	54 Мбіт/с (2,4 ГГц); До 6,77 Гбіт/с (5 ГГц)
Радіус дії	10-100 м	10 м	40 км	100м (2,4ГГц)
Номінальна потужність	(-25)-0 дБм	0-10 дБм	43 дБм	15-20 дБм
Кількість радіоканалів	1/10;16	79	–	14(2,4 ГГц)
Ширина каналу	0,3/0,6 МГц; 2МГц	1 МГц	1,25-20 МГц	22 МГц

Продовження таблиці1.1

	ZigBee	Bluetooth	WiMax	Wi-Fi
Шифрування	128 AES, CBC	E0, ECB	AES , 3DES,	AES і RS4,

			ECB	CBC
Енергоспоживання	Низьке	Середнє	Дуже високе	Високе
Автентифікація користувача	Немає	Немає	Parol	TKIP
Підтримка хендоверу	Є	Є	Є	Є
Можливість передачі великого об'єму даних	Немає	Є	Є	Є

Виходячи із приведеного вище опису технологій та посилаючись на пункт 1.4, можна порівняти технології та вибрати відповідну. Забезпечити надійним радіо покриттям можливо використовуючи технології ZigBee, WiMax та Wi-Fi, Bluetooth в свою чергу має надто малий радіус дії. Кожна із технологій підтримує можливість хендоверу. Не менш важливою вимогою є підтримка передача даних різних форматів, включаючи потокове аудіо- та відео повідомлення та VoIP телефонію. Лише WiMax та Wi-Fi мають змогу забезпечити передачу даних цих форматів. Виходячи із цього ZigBee та Bluetooth не мають можливості забезпечити обмін достатньо великими об'ємами інформації. З огляду на безпеку системи найбезпечнішими є технології Wi-F і WiMax. Автентифікація – основа безпеки будь-якої системи, яка полягає в перевірці достовірності даних про користувача сервером. Відсутність автентифікації може призвести до неконтрольованого доступу до цієї мережі. Тому, відсутність автентифікації в ZigBee та Bluetooth є значним мінусом з точки зору безпеки. Також, стандарти шифрування надійніші у WiMax та Wi-Fi. З економічної точки зору найоптимальнішими технологіями є ZigBee, Wi-Fi та Bluetooth. Вони використовують не ліцензовані діапазони частот, тобто немає необхідності витрачати кошти на придбання ліцензії. В той час як WiMax використовує не ліцензовану смугу частот 2,4 ГГц та 5 ГГц, переважна більшість інших

частот на яких працює WiMax потребує придбання ліцензії. Але найголовнішим недоліком WiMax є складність розгортання, а відповідно і складність модернізації та розширення мережі, в той час такого недоліку у решти технологій немає. Останнім критерієм вибору є енергоспоживання. Технології ZigBee та Bluetooth мають найнижчі показники споживання енергії, в той час як WiMax має високі показник енергоспоживання, Wi-Fi займає проміжну ланку, що є допустимим при проектуванні мережі.

Отже, порівнюючи технології можна сказати, що лише технологія Wi-Fi відповідає усім вимогам, які були приведені в пункті 1.4. Важливо додати, що на основі цієї технології є вже побудовані мережі в будівлі третього корпусу. Саме через це мережу не потрібно будувати, її необхідно лише модернізувати. Тому це ще одна перевага у використанні Wi-Fi.

2 ВИБІР СТАНДАРТУ ТА ПРОЄКТУВАННЯ МЕРЕЖІ

2.1 Вибір стандарту технології Wi-Fi для реалізації проєкту

Wi-Fi налічує 30 стандартів. Тому після вибору технології, необхідно вибрати відповідний стандарт цієї технології. Тут треба звернути увагу на те, що спочатку при розробці стандартів сімейства IEEE 802.11, їх розробники були переконані в тому, що абонентські пристрої можуть рухатися тільки навколо однієї фіксованої точки доступу. Але життя показало, що розвиток телекомунікацій та фінансова доступність мережі Wi-Fi призводить до необхідності побудови мереж, які покривають певну площу і складаються з декількох точок доступу, що розташовуються на відстані дії одна від одної. Звісно, такі мережі потребують автоматичної передачі обслуговування абонентів із зони дії однієї точки доступу до зоні дії іншої. Тому головним критерієм вибору є підтримка режиму хендоверу в технології Wi-Fi. Зазначимо, що хендовер (англ. Handover – передавати) – це режим роботи мобільної станції, точок доступу Wi-Fi та комутаційного обладнання, при якому виконується весь комплекс процедур естафетної передачі працюючої станції від однієї фіксованої точки доступу до іншої.

Розглянемо три з можливих основних стандартів технології Wi-Fi, які підтримують цю функцію.

2.1.1 Стандарт IEEE 802.11i

IEEE 802.11i – це стандарт для бездротових локальних мереж (WLAN), який забезпечує поліпшене шифрування для мереж. Стандарт 802.11i вимагає нових протоколів ключів шифрування, відомих як протокол інтеграції тимчасового ключа (TKIP) і розширений стандарт шифрування (AES).

Функціями 802.11i є кешування ключів, яке полегшує повторне підключення до мережі для користувачів, які тимчасово відключилися, і попередня автентифікація, яка забезпечує швидке відновлення цього підключення.

Архітектура 802.11i містить два наступні компоненти: 802.1X для автентифікації, RSN (Robust Security Network) для відстеження асоціацій, і CCMP (Counter Mode with Cipher Block Chaining Message Authentication Protocol), який базується на алгоритмі шифрування AES. Іншим важливим елементом процесу автентифікації є чотиристоронне рукостискання (4-Way Handshake) – протокол керування ключами 802.11i.

Для прискорення безпечного роумінгу 802.11i містить дві властивості, які спрямовані на традиційні точки доступу (ТД), що працюють незалежно, а не спільно з комутатором WLAN:

а) кешування парного майстер-ключа (PMK) дозволяє клієнтові асоціюватися з точкою доступу і, після виконання повної автентифікації RADIUS, зберегти майстер-ключ, узгоджений з цією точкою доступу, в кеші. Якщо користувач піде від цієї точки доступу і повернеться назад, клієнтові не доведеться проходити повторну автентифікацію;

б) преавтентифікація або "швидка асоціація заздалегідь". Використовуючи цю можливість, визначену стандартом 802.11i, точка доступу 802.11, що пов'язана з клієнтом, може встановити міст до інших точок доступу через дротову мережу і попередньо автентифікувати клієнта на "наступній" точці доступу, до якої клієнт може переміщатися [10].

При кожній асоціації клієнт-ТД – незалежно від того, чи використовується кешування попарного майстер-ключа (PMK Caching або PKC) – стандарт 802.11i передбачає отримання парного перехідного ключа (PTK) через чотиристоронне рукостискання, яке захищає дані, фактично передані по повітрю. PTK скидається кожен раз, коли користувач

переміщується із зони дії ТД до якої він був підключений. Якщо РТК не працює, потрібна повторна автентифікація.

Головним недоліком цього стандарту є те, що швидке перепідключення користувача відбувається лише за тієї умови, якщо користувач раніше вже проходив повну процедуру автентифікації в цій точці доступу.

Рисунок 2.1 – Хендовер в стандарті 802.11i

2.1.2 Стандарт IEEE 802.11v

802.11v (Basic Service Set Transition Management) – це стандарт управління переходом набору базових послуг (або скорочено BSS), також відомого як перехід від однієї точки доступу до іншої. 802.11v дозволяє

клієнтським пристроям обмінюватися інформацією про топологію мережі, включаючи інформацію про радіочастотне середовище.

802.11v описує удосконалення в управлінні бездротовою мережею, такі як:

– енергозбереження за допомогою мережі – допомагає клієнтам продовжити термін служби батареї, дозволяючи їм довше знаходитись в режимі сну;

– хендовер в мережі – дозволяє WLAN відправляти повідомлення пов'язаним клієнтам, щоб точки доступу могли краще зв'язуватися з клієнтами. Це корисно як для балансування навантаження, так і для направлення клієнтів з поганим підключенням до іншої ТД.

В рамках BSS Transition існує 3 типи повідомлень, це запит від клієнта на вказівку відповідних точок доступу, і два повідомлення від точки доступу. В разі якщо точка доступу перевантажена, і просить клієнта перейти на іншу, то надсилається повідомлення Load Balancing Request, а якщо параметри індикатора рівня сигналу, що приймається (RSSI) і швидкість передачі даних (Data Rate) не задовольняють мінімальним вимогам ТД, тоді надсилається Optimized Roaming Request. Тут важливо відзначити, що це рекомендаційні повідомлення, і дії залишаються на розсуд клієнта. Примусове відключення від ТД можливе тільки в рамках технологій Band/Load Steering/Balancing, і може бути некоректно відпрацьовано клієнтом, або зовсім проігноровано.

Тобто недоліком стандарту 802.11v є те, що рішення про перехід до іншої точки доступу не є примусовим, тільки клієнт може прийняти рішення про переключення до іншої ТД.

2.1.3 Стандарт IEEE 802.11r

802.11r також відомий, як швидка передача (FT – Fast Transition) – це стандарт IEEE для швидкої безпечної передачі мобільної станції (МС) між

точками доступу. Він представляє нову концепцію хендоверу для технології Wi-Fi, в якій початкове "рукостискання" МС з новою ТД виконується ще до того, як клієнт перейде до стійкої зони дії цільової точки доступу. Початкове "рукостискання" дозволяє клієнту і ТД зробити наступний розрахунок парного перехідного ключа (PTK) заздалегідь. Ці ключі PTK застосовуються до МС клієнта і ТД після того, як клієнтська МС зробить запит на повторне асоціювання або обмін відповідями з новою цільовою ТД.

Основна перевага 802.11r полягає в значному скороченні часу за рахунок того, що ієрархія ключів FT розроблена для того, щоб клієнтські МС могли здійснювати швидкі переходи від однієї точки доступу до іншої без необхідності повторної автентифікації в кожній точці доступу. Також 802.11r усуває більшу частину накладних витрат на квитування при переході, і тим самим скорочуючи час передачі даних між точками доступу, що забезпечує більш надійну безпеку і QoS. У строго захищеної WLAN (в тій, яка використовує методи шифрування 802.1x та EAP), але без 802.11r, мобільний пристрій має буде пройти повну повторну автентифікацію після повторної асоціації. Це може викликати суттєве переривання медіапотоку. Але з 802.11r повторна автентифікація ефективно виконується до повторної асоціації (фактично встановлюючи «перервати перед перериванням», а не «перервати перед включенням»).

Ще додатковою перевагою є те, що без повторної автентифікації між WLAN і сервером автентифікації AAA (Authentication, Authorization and Accounting) генерується набагато менше трафіку, що в свою чергу покращує як масштабованість, так і з'єднання між WLAN і сервером автентифікації.

Все це особливо корисно для клієнтських пристроїв, які мають чутливі до затримок програми та використовують інтерактивні сервіси в реальному часі (наприклад, голос і відео) [11].

Таким чином за допомогою всіх трьох описаних вище стандартів можна здійснювати процедуру хендоверу в мережі, яка використовує

технологію Wi-Fi. Але враховуючи всі недоліки і переваги серед запропонованих трьох варіантів найоптимальнішим варіантом для даного проєкту буде використання стандарту 802.11r.

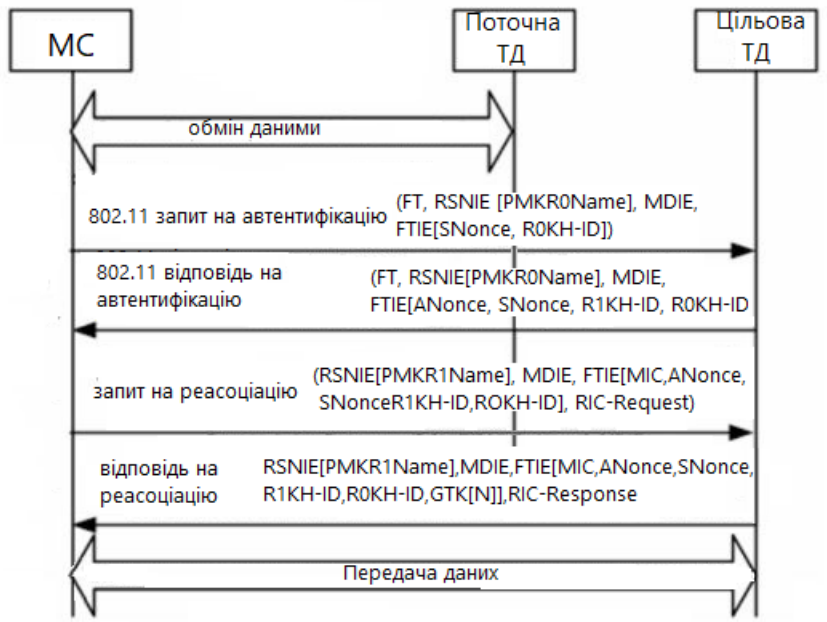

Рисунок 2.2 – Процес хендоверу в стандарті 802.11r

2.2 Хендовер в бездротових мережах та стандарті 802.11r

В загалі в мобільному зв’язку хендовер – це процес, який підтримує безперервність виклику або сеанс зв'язку мобільної станції при переміщенні в зону покриття і із зони покриття різних стільників. Це досягається шляхом перемикання поточного каналу в поточному стільнику на новий канал, коли МС переміщається до нового стільника.

В цілому, в мобільному зв’язку процедура передачі складається з трьох фаз:

– перша фаза – вимірювання. Результатом цієї фази є звіт про вимірювання із використаними критеріями вимірювання;

– друга фаза – це рішення про здійснення хендоверу. Зазвичай виконується алгоритмами хендоверу з параметрами алгоритму та критеріями хендоверу, як вхідними даними;

– третя фаза – це процес виконання хендоверу, в ході якого новий канал буде призначений МС, а старе з'єднання буде перервано.

З точки зору з’єднання хендовер можна розділити на два класи:

– жорсткий хедовер;

– м’який хендовер.

В першому випадку існуюче з’єднання розривається до встановлення нового. В другому випадку з'єднання з попередньою точкою доступу розривається тільки після встановлення з'єднання з наступною доступною.

Основні вимоги до хендоверу:

– час затримки хендоверу повинен бути низьким. Передача має бути досить швидкою, щоб користувач не міг виявити жодного погіршення обслуговування або переривання під час хендоверу;

– вплив передачі обслуговування на QoS повинен бути мінімальним. Наприклад: ймовірність переривання поточного виклика повинна бути мінімізована, а трафік між сусідніми стільниками повинен бути збалансований [12].

Далі мова піде про процес хендоверу в бездротових локальних мережах.

В стандарті 802.11 хендовер виконується на канальному рівні і містить в собі три фази:

Перша фаза – виявлення. Процес виявлення може бути або активним, або пасивним. При пасивному скануванні МС слухає широкомовний сигнал радіомаяка, який періодично посилається точками доступу. В активному скануванні, МС активно надсилає запит на зондування Probe Request до точки доступу. Кожна точка доступу, яка отримала запит, відповість на нього.

Друга фаза – це повторна автентифікація. На цій фазі МС автентифікується з найкращою за параметрами точкою доступу, знайденою в першій фазі.

Третя фаза – це асоціація. Як тільки МС автентифікувалась з новою ТД, МС надсилає запит на реасоціацію з новою ТД. У відповідь нова ТД надсилає відповідь на запит, який містить в собі інформацію про швидкість передачі даних, ID станції і т.д.

Оскільки вибраним стандартом в бездротовій локальній мережі є 802.11r, то нижче описана процес хендоверу саме для цього стандарту.

Мобільний домен (BSS) включає кілька точок доступу в межах автономної системи (ESS). Точки доступу в в межах BSS повинні координувати свою роботу один з одним, обмінюватися інформацією про бездротових клієнтів, включаючи майстер-ключ PMK (Pairwise Master Key). Для прискорення процесу перемикання застосовується, попередня автентифікація клієнта до безпосереднього початку процесу перепідключення.

Перша точка доступу, на якій станція проходить автентифікацію, буде кешувати свій PMK використовуючи його для отримання сеансових ключів для інших точок доступу. Ця точка доступу має назву R0 Key Holder (R0KH), так як вона має рівень 0 PMK(PMK-R0). Коли MS повторно зв'язується з новою точкою доступу, R0KH генерує PMK-R1 та передає його новій точці доступу, яка називається R1KH. Нова точка доступу взаємодіє скоріше з R0KH, чим безпосередньо із сервером AAA.

Для того, щоб клієнт зміг перейти від однієї точки доступу до наступної з використанням протоколів FT, обмін повідомленнями відбувається за допомогою одного з наступних двох методів:

– over-the-Air FT Roaming;

– over-the-DS (Distribution System) FT Roaming.

Over-the-Air FT Roaming – по повітрю клієнт взаємодіє з точкою доступу, до якої він повинен підключитися перед початком міграції. Нижче описана процедура хендоверу (рис.2.3):

а) клієнт пов'язаний з ТД1 і хоче здійснити хендовер до ТД2;

б) клієнт надсилає запит на автентифікацію FT до ТД2 і отримує відповідь на автентифікацію FT від ТД2;

в) клієнти надсилає запит на з’єднання до ТД2 і отримують відповідь на з’єднання від ТД2;

г) клієнт завершує хендовер від ТД1 до ТД2.

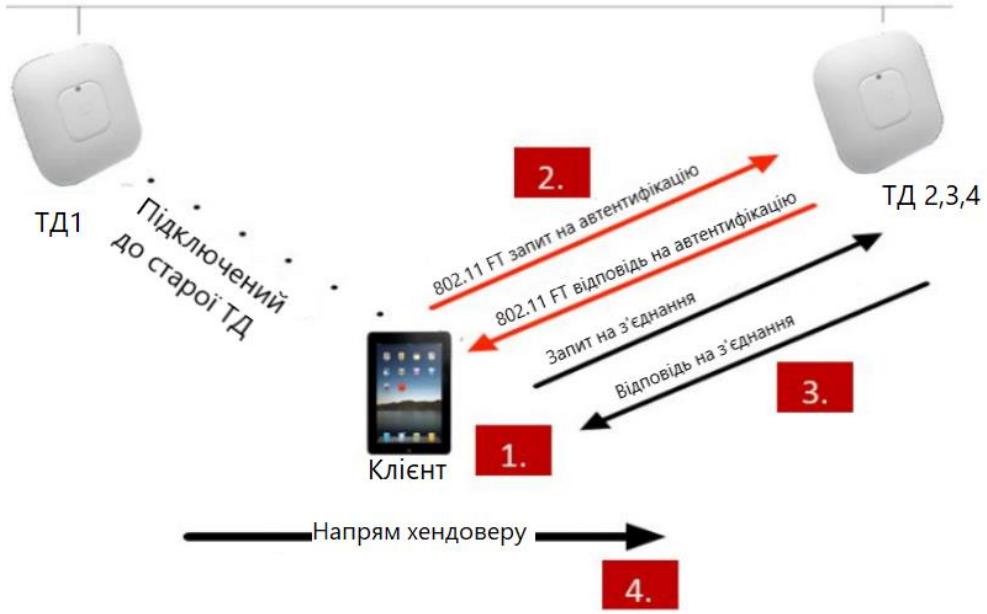

Рисунок 2.3 – Процедура хендоверу Over-the-Air

Over-the-DS (Distribution System) FT Roaming – клієнт взаємодіє з точкою доступу, до якої він повинен підключитися перед початком міграції, через точку доступу, до якої він підключений в поточний момент часу. Нижче описана процедура хендоверу (рис.2.4):

а) клієнт під’єднаний до ТД1 і хоче здійснити хендовер до ТД2;

б) клієнт надсилає запит на автентифікацію FT до ТД1 і отримує відповідь на автентифікацію FT від ТД1;

в) точки доступу підключені до одного контролера, отже інформація про попередню автентифікацію надсилається з контролер до ТД2;

г) клієнт надсилає запит на з’єднання до ТД2 і отримує відповідь на з’єднання від ТД2 [13].

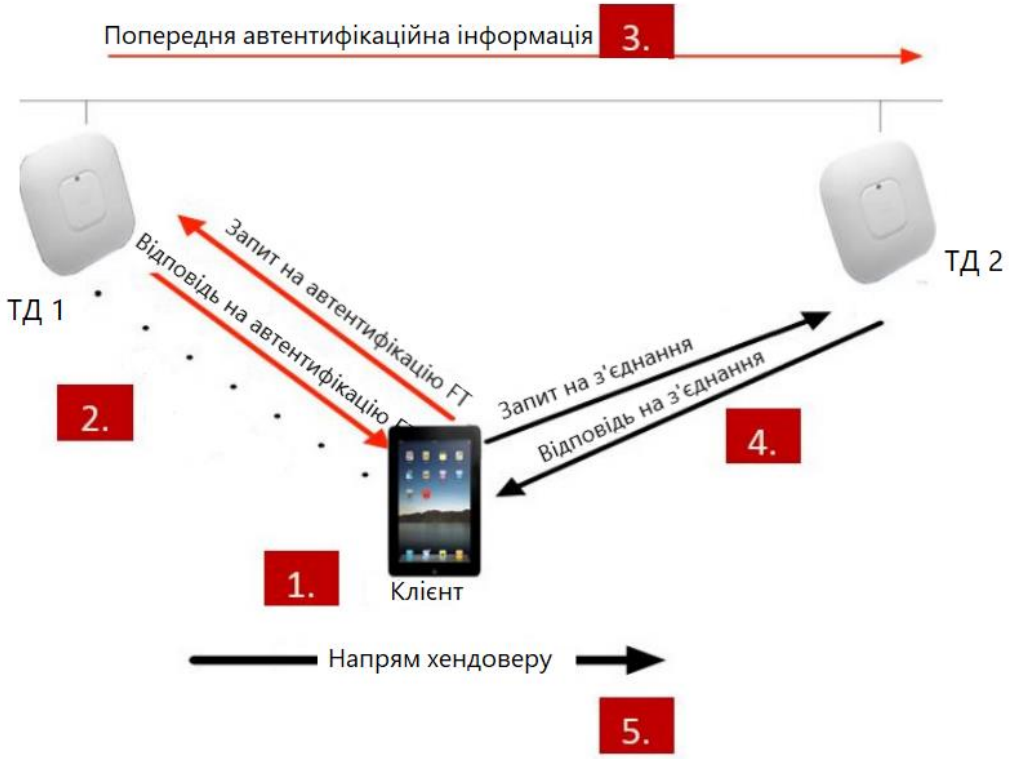

Рисунок 2.4 – Процедура хендоверу Over-the-DS

2.3 Проєктування мережі

Виходячи з основних вимог до проектованої мережі (глава 1) проєктована мережа буде будуватися на основі централізованої архітектури. Для такої архітектури мережі Wi-Fi характере повне управління інфраструктурою мережі радіо доступу, яке виконується контролером мережі WLAN. Такий контролер в централізованій мережі стандарту Wi-Fi управляє:

хендовером клієнтів між різними точками доступу в зоні їх покриття; завантаженням/зміною ПО; змінами конфігурації; RRM (динамічне управління радіоресурсами); керує зв'язком мережі WiFi-стандарту з зовнішніми серверами (AAA, DHCP, LDAP і т.п.); керує автентифікацією користувачів; керує профілями якості обслуговування QoS, спеціальними функціями і т.п. Більш того, є випадки коли для об’єднання декілька тисяч ТД такі контролери об'єднуються в групи (домени) для забезпечення безшовного переходу клієнтів між усіма точками доступу [14].

Враховуючи об’єм мережі навчального корпусу університету можуть бути запропоновані два варіанти побудови цієї архітектури: побудова на основі віртуального контролера або на основі апаратного контролера мережі. Віртуальний контролер означає використання звичайної точки доступу, яка бере на себе ще функції контролера. У випадку використання апаратного контролера весь трафік та дані, необхідні для керування мережею, проходять безпосередньо через контролер. Це означає, що під час великих навантажень, контролер може не впоратись з навантаження та призвести до збою в мережі. Через віртуальний контролер проходять лише дані для керування: автентифікація, координація сесій, запобігання вторгнень, керування радіо покриттям і т.д. Інший трафік в таких мережах оминає контролер і передається в мережу напряму. Але не зважаючи на переваги віртуального контролера, його недоліком є складність модернізації вже існуючої мережі. Оскільки метою проєктованої мережі є не створення, а модернізація її, то пропонується використання апаратного контролеру.

Для того, щоб об’єднати точки доступу та контролер в одну мережу їх необхідно з’єднати між собою. Існує два варіанти об’єднання:

– з’єднання за допомогою крученої пари;

– з’єднання за допомогою Wi-Fi.

Перший спосіб є найнадійнішим і найстабільнішим, але недоліком є складність прокладання кабелю та можлива висока вартість. Другий спосіб є

значно простішим і менш витратним, але при цьому швидкість і надійність мережі знижується.

З урахуванням того, що будівля, для якої проєктується мережа має п’ять поверхів, на яких вже існує мережа Ethernet, то кращим варіантом є використання крученої пари для забезпечення надійним радіо покриттям на всіх поверхах.

На основі даних про планування будівлі та інформації, яка була описана вище, нижче на рисунку 2.**5** наведено схемне рішення проєктованої мережі для третього поверху.

На рисунку синім кольором показані вже існуючі точки доступу, сірим – додані відповідно до модернізації мережі, чорним кольором показаний контролер, синім – кручена пара.

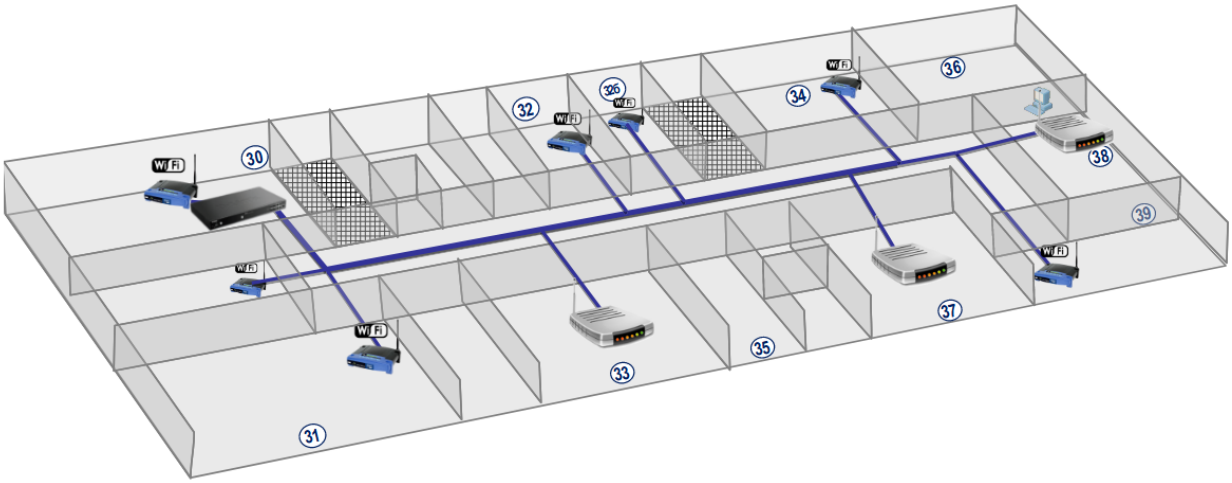

Рисунок 2.5 – Схема модернізованої мережі для третього поверху

Із рисунка 2.5 видно, що мережа має централізовану архітектуру, всі точки доступу підключені до апаратного контролера за допомогою крученої пари.

3 РОЗРАХУНОК КІЛЬКОСТІ ТОЧОК ДОСТУПУ ТА ВИБІР ОБЛАДНАННЯ

3.1 Розрахунок кількості потенційних абонентів в корпусі

Вибравши необхідний стандарт та архітектуру мережі, необхідно визначити кількість потенціальних абонентів, які перебувають в будівлі одночасно. Це необхідно для того, щоб в подальшій роботі було можливим розрахувати кількість точок доступу та кількість користувачів на одну точку доступу.

Усі дані зібрані шляхом статистичних досліджень в період з 1 вересня по 30 вересня. Розрахунок кількості потенціальних абонентів проводився шляхом підрахунку максимальної кількості місць в аудиторіях та приміщеннях кафедр. Такий розрахунок проводиться для того, щоб під час заповнення аудиторії на 100% мережа була здатна впоратись з навантаженням.

Тут ще необхідно звернути увагу на те, що майже на кожному поверсі навчального корпусу є свої комп’ютерні класи, які в свою чергу підключені до виходу в інформаційну мережу, тому немає крайньої потреби встановлювати в цих аудиторіях точки доступу, але все одно необхідно забезпечити надійним радіо покриттям.

Як відомо із пункту 1.3, на першому поверсі знаходиться 4 аудиторії. Кожна з цих аудиторій може вмістити 25-30 чоловік. В загальному підрахунку на першому поверсі під час навчального процесу знаходиться 120 чоловік. Також необхідно врахувати знаходження потенціальних абонентів не тільки в предметних аудиторіях, а і в інших кімнатах. Наприклад адміністративні приміщення кафедри та викладацькі. Отже за загальним рахунком на поверсі знаходиться приблизно 130-135 чоловік. Впродовж збору статистичних даних кількість людей на поверсі не перевищувала 135.

На другому поверсі знаходиться вісім аудиторій. Дві із цих аудиторій можуть одночасно вмістити 40 чоловік. Три аудиторії мають вмістимість 20 чоловік. Решта аудиторій вміщує 15 чоловік. З урахування користувачів, які не знаходяться в предметних аудиторіях на поверсі перебуває 195 чоловік. Впродовж збору статистичних даних кількість людей не перевищувала 195.

Третій поверх складається з восьми аудиторій. Кожна аудиторія в середньому може вмістити 20 до 25. З урахування користувачів, які не знаходяться в предметних аудиторіях на поверсі перебуває 230 чоловік. Але, необхідно зауважити, що на поверсі знаходиться дві аудиторії оснащені комп'ютерами, які мають доступ до інформаційної мережі. Тобто користувачам немає необхідності використовувати бездротову мережу. Саме через це рахується, що із 20 користувачів, які знаходяться в комп'ютерних аудиторіях, користуються бездротовою мережею лише 5. Отже в загальному підрахунку потенційних користувачів налічується 200. Впродовж збору статистичних даних кількість людей не перевищувала 200.

Четвертий поверх складається з семи аудиторій. Кожна аудиторія в середньому може вмістити від 20 до 25 чоловік. З урахування користувачів, які не знаходяться в предметних аудиторіях на поверсі перебуває 205 чоловік. Але, необхідно зауважити, що на поверсі знаходиться дві аудиторії оснащені комп'ютерами, які мають доступ до інформаційної мережі. Тобто користувачам немає необхідності використовувати бездротову мережу. Саме через це рахується, що із 20 користувачів, які знаходяться в комп'ютерних аудиторіях, користуються бездротовою мережею лише 5. Отже в загальному підрахунку потенційних користувачів налічується 175. Впродовж збору статистичних даних кількість людей не перевищувала 175.

П’ятий поверх складається з семи аудиторій. Кожна аудиторія в середньому може вмістити від 20 до 25 чоловік. З урахування користувачів, які не знаходяться в предметних аудиторіях на поверсі перебуває 205 чоловік. Але, необхідно зауважити, що на поверсі знаходиться дві аудиторії

оснащені комп'ютерами, які мають доступ до інформаційної мережі. Тобто користувачам немає необхідності використовувати бездротову мережу. Саме через це рахується, що із 20 користувачів, які знаходяться в комп'ютерних аудиторіях, користуються бездротовою мережею лише 5. Отже в загальному підрахунку потенційних користувачів налічується 200. Впродовж збору статистичних даних кількість людей не перевищувала 175.

Результати досліджень кількості користувачів по поверхам наведені в таблиці 3.1.

Таблиця 3.1 – Розрахунки кількості користувачів по поверхам корпусу

Поверх	Кількість предметних аудиторій (без комп'ютерних класів)	Вмістимість аудиторії (корист.)	Кількість користувачів в адмін. приміщеннях кафедр	Загальна кількісь користувачів на поверсі
1	4	25-30	15	135
2	2	40	40	195
	3	20		
	3	15		
3	8	20-25	30	200
4	7	20-25	30	175
5	7	20-25	30	175

Отже, підрахувавши усереднену кількість на кожному поверсі, можна сказати, про загальну кількість людей, які перебувають в споруді одночасно. Кількість становить в середньому 855-860 чоловік.

Наступним кроком після підрахунку загальної кількості людей постає необхідність в розрахунку максимальної кількості людей для однієї точки доступу.

3.2 Розрахунок кількості користувачів на одну точку доступу

До точки доступу Wi-Fi можна одночасно підключити велику кількість клієнтських пристроїв. Число підключених користувачі може варіюватися від 1 до декількох тисяч. Точна цифра залежить від обмежень пристрою. Однак, в більшості випадків підключати таке велике число клієнтів не рекомендується з огляду на особливості роботи самого протоколу Wi-Fi. Все це обумовлюється тим, що призначені для користувача пристрої на кшталт ноутбуків, смартфонів і так далі працюють саме по якомусь стандарту з усього сімейства 802.11 і вони не можуть підтримувати спеціально створені механізми і протоколи для прискорення роботи радіочастини. Без таких протоколів і механізмів, коли підключено велику кількість клієнтів, сумарна швидкість передачі даних різко знижується через те, що відбувається ділення між усіма підключеними клієнтами до однієї ТД.

Одним з найпростіших способів визначення кількості точок доступу є задання фіксованої кількості користувачів на точку. Із пункту 1.1 відомо, що один користувач споживає до 2,4 Мб/год або 5,5 Мбіт/с. Якщо рахувати, що кожен з 20 користувачів використовує Zoom для on-line конференції в один момент часу, то використовуваний трафік становить 110-150 Мбіт/с. Якщо використовувати точку доступу з підтримкою стандарту 802.11n (максимальна пропускна здатність до 600 Мбіт/с), то цілком вдасться задовольнити потреби кожного з користувачів. Якщо ТД має низку пропускну здатність, то відповідно кількість підключених користувачів повинна бути меншою.

3.3 Розрахунок кількості точок доступу

Наступним етапом є розрахунок необхідної кількості точок доступу. Розрахунок буде проводитись на прикладі для третього поверху навчального корпусу:

– N = 200 – максимальне число користувачів, що одночасно працюють в мережі;

– F = 2 Мбіт/с – необхідна гарантована швидкість для одного користувача;

– D_T = 0,65 – частка планшетів і смартфонів в мережі;

– D_L = 0,35 – частка ноутбуків в мережі;

– $D_{2.4\ ГГц}$ = 0,6 – частка пристроїв, що працюють в діапазоні 2,4 ГГц.

– $D_{5\ ГГц}$ = 0,4 – частка пристроїв, що працюють в діапазоні 5 ГГц.

Смартфони та планшети використовують 20 МГц канал в один потік, що забезпечує теоретичну швидкість роботи 72 Мбіт/с. Реальна швидкість при цьому буде приблизно в два рази менше і буде дорівнювати F_T = 35 Мбіт/с.

Ноутбуки використовують 20 МГц канал в два потоки, що забезпечує теоретично швидкість роботи 144 Мбіт/с. Реальна швидкість при цьому буде дорівнювати приблизно в два рази менше і буде дорівнювати F_L = 70 Мбіт / с.

Тепер визначимо коефіцієнт ефірного часу (airtime) для кожного з типів пристроїв.

$$\text{À} = \frac{F}{F_T} = 0.0571, \tag{3.1}$$

$$\text{A} = \frac{F}{F_L} = 0.0286 \tag{3.2}$$

Загальний коефіцієнт ефірного часу для всіх пристроїв кожного типу буде дорівнювати:

$$A_T^{заг} = A_T \cdot N \cdot D_T = 7.423, \quad (3.3)$$

$$A_L^{заг} = A_L \cdot N \cdot D_L = 2,002 \quad (3.4)$$

Загальний коефіцієнт ефірного часу з урахуванням службового трафіку буде дорівнювати:

$$A = \left(A_T^{заг} + A_L^{заг}\right) \cdot 1.25 = 11.781 \quad (3.5)$$

Далі необхідно визначити кількість радіомодулів, що працюють в діапазоні 2,4 ГГц, і радіомодулів, що працюють в діапазоні 5 ГГц:

$$N_{2.4ГГц} = (A \cdot D_{2.4ГГц}) = 7, \quad (3.6)$$

$$N_{5ГГц} = (A \cdot D_{5ГГц}) = 5 \quad (3.7)$$

Таким чином, для організації бездротової мережі потрібно або 7 точок доступу, що працюють в діапазоні 2,4 ГГц, і 5 точки доступу, що працюють в діапазоні 5 ГГц, або 7 дводіапазонних точок доступу 2,4/5 ГГц з можливістю одночасної роботи в обох діапазонах.

Хоча цей розрахунок є достатньо точним, але він не враховує місцевість на якій будуть розташовані ТД. При розміщенні точок доступу дуже важливо визначити, з яких матеріалів зроблені стіни, перекриття, конструкційні елементи і меблі в приміщенні, і вже з урахуванням цього проводити

розміщення обладнання, які будуть використовуватися разом з точками доступу. Саме через це запропонованим варіантом розрахунку кількості точок доступу, який буде все це враховувати є використання програми Wi-Fi Planner Pro [15].

3.4 Моделювання в програмі D-Link Wi-Fi Planner Pro

Як згадувалось вище, для найбільш точного розрахунку необхідно врахувати місцевість, матеріали стін і т. і. Для цього пропонується використання програми D-Link Wi-Fi Planner Pro. Програма D-Link Wi-Fi Planner Pro призначена для первинного аналізу плану приміщення з метою розміщення на ньому точок доступу Wi-Fi. Програма орієнтована на використання обладнання D-Link.

З пункту 3.3 було визначено, що необхідна кількість ТД – 7 штук. Оскільки мережа модернізується, то необхідно враховувати вже існуючі ТД. На третьому поверсі вже розташовано 7 точок доступу. Тому на рисунку 3.1 зображено вже існуючі токи доступу та їх розміщення.

Із рисунку 3.1 видно, що точки доступу покривають всю площу третього корпусу, але на деяких ділянках рівень сигналу дорівнює -75 дБм. Вважається, що для доступу в Інтернет (електронна пошта та веб-серфінг) необхідно забезпечити на всій території приміщення рівень сигналу не гірше, ніж -(68-70) дБм. Саме через це постає питання щодо покриття всієї необхідної площі необхідним рівнем сигналу. Існує два можливих варіанти вирішення проблеми.

Перший варіант – це додавання ще однієї точки доступу в аудиторію 35 як це зображено на рисунку 3.2.

Із рисунку видно, що необхідна територія покрита на 100%. Також рівень потужності сигналу на кожній ділянці дорівнює не менше ніж -60 дБм.

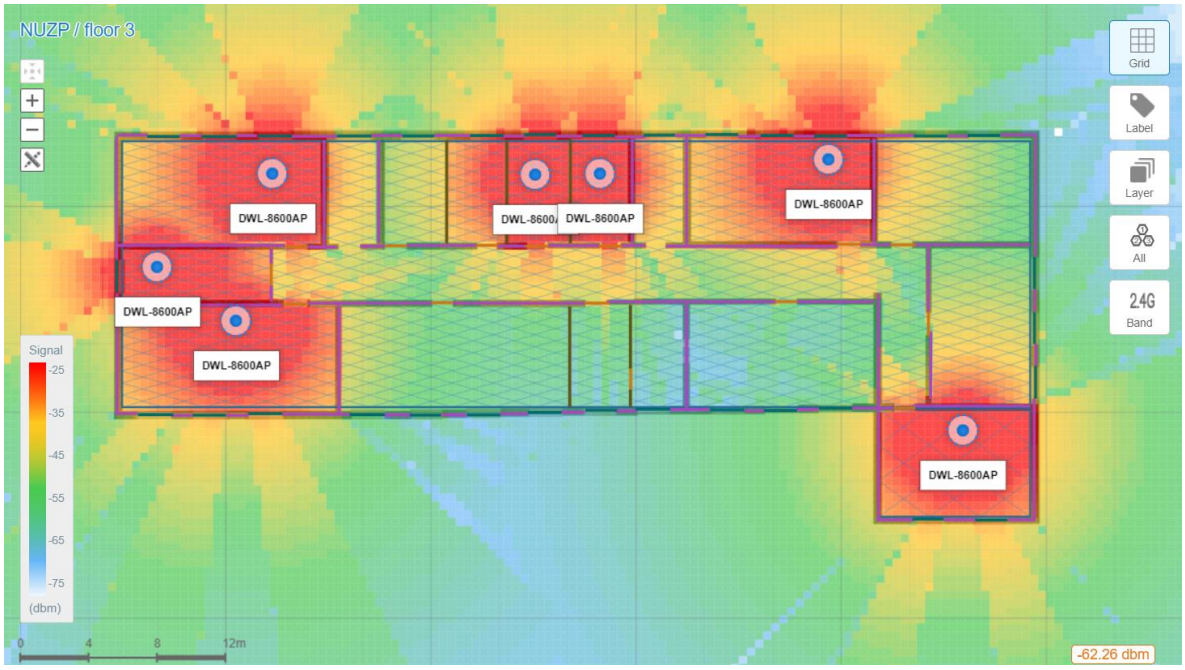

Рисунок 3.1 – Розміщення існуючих точок доступу

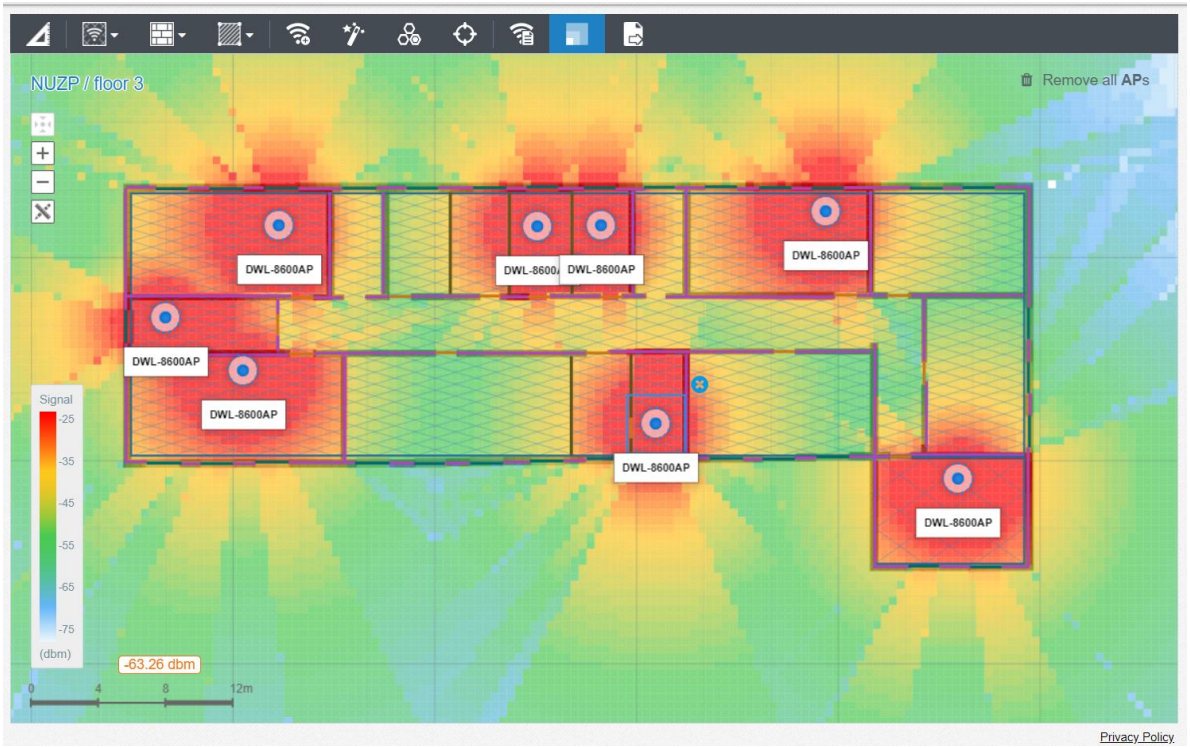

Рисунок 3.2 – Розміщення наявних і додаткової точок доступу

Другим запропонованим варіантом є розміщення вже існуючих точок доступу таким чином щоб вдавалось досягти надійного радіо покриття на всій необхідній площі (рис. 3.3).

Із рисунку видно, що площа всього поверху покрита на 100%. Також рівень потужності сигналу є не менше ніж -60 дБм.

Отже, під час підрахунку було визначено, що необхідна кількість точок доступу на третій поверх дорівнює 7, моделювання в програмі показало, що 7 точок доступу є оптимальним варіантом.

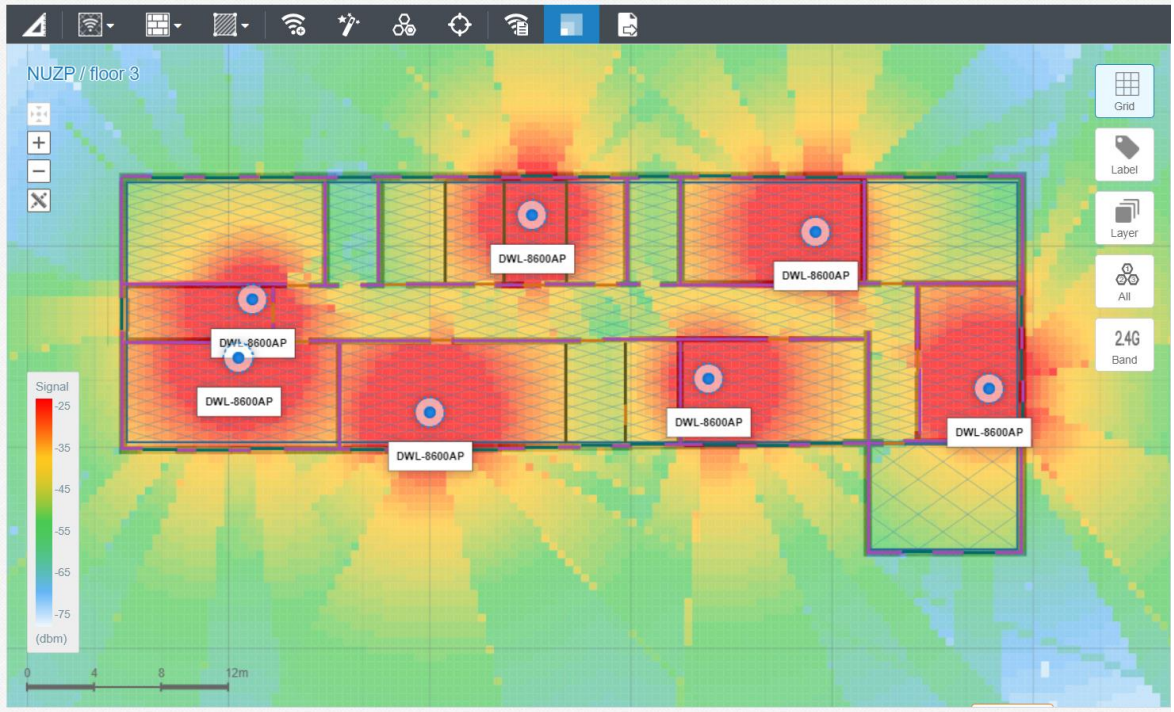

Рисунок 3.3 – Запропоноване розміщення ТД

Важливо звернути увагу на те, що існуючі точки доступу мають підтримувати стандарт 802.11r. Якщо існуюча точка доступу не підтримує цей стандарт, то здійснення хендоверу буде неможливим. Запропонованим варіантом вирішення проблеми є встановлення точки доступу, яка підтримує цей стандарт.

3.5 Вибір обладнання

Після того як було зроблено розрахунок необхідної кількості точок доступу і відтворено в стимуляційний програмі, наступним кроком є вибір обладнання. Необхідними пристроями є контролер бездротової мережі та точки доступу. Вибір буде проводитись серед моделей компанії D-Link.

При виборі контролера до нього висувається ряд вимог. З урахуванням того, що метою проектованої мережі є забезпечення хендовером, то найголовнішим критерієм вибору обладнання є підтримка стандарту 802.11r. А також, можливість підключення до 64 точок доступу.

Серед представленого обладнання найбільш відповідною до критерієв є DWL-6620APS. Нижче наведені характеристики.

Бездротовий контролер DWC-1000 (рис.3.4) здійснює централізоване управління пристроями в бездротовій мережі LAN. Пристрій є повнофункціональним і економічним рішенням для мереж малого і середнього бізнесу завдяки можливості управління від 12 до 66 бездротовими точками доступу. Функції автоматичного виявлення точок доступу і централізованого управління. Завдяки надійній і багатофункціональної системи безпеки DWC-1000 забезпечує захист від потенційних атак неавторизованих користувачів і пристроїв в бездротової мережі.

Процесор – Cavium 7020.

Оперативна пам’ять – 1024 МБ, DDR II.

Кількість користувачів, які одночасно можуть проходити автентифікацію на адаптивному порталі – 1024

Стандарти: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab.

Підтримка стандарту 802.11r – є.

Моделі керуємих ТД: DWL-8720AP, DWL-8620AP, DWL-8710AP, DWL-8610AP, DWL-7620AP, DWL-6700AP, DWL-6620APS, DWL-6610AP, DWL-3610AP, DWL-2600AP.

Рисунок 3.4 – Бездротовий контролер DWC-1000

Із характеристик видно, що дана модель задовольняє всім вимогам. Є підтримка стандарту 802.11r, можливість підключення до 64 точок доступу.

Далі розглядається вибір точки доступу. Найголовнішими критеріями вибору обладнання є підтримка стандарту 802.11r. Також, необхідно, щоб точки доступу були двох діапазонними. Із пункту 3.3 було розраховано кількість точок доступу, яка дорівнювала 7 точок доступу в діапазоні 2,4 ГГц і 5 точок доступу в діапазоні 5 ГГц або використання 7 ТД, які працюють в двох діапазонах. З економічною точки зору кращим варіантом є використання останнього варіанту. Бажано, щоб ТД підтримувала стандарт 802.11n, для забезпечення високою пропускною здатністю. Вибрана модель має бути уніфікована з бездротовим контролером DWC-1000. Серед представленого обладнання найбільш відповідною до критеріїв є DWL-6620APS. Нижче наведені характеристики.

Уніфікована бездротова точка доступу D-Link DWL-6620APS призначена для організації масштабованих бездротових мереж на підприємствах малого та середнього бізнесу. DWL-6620APS підтримує одночасну роботу в двох діапазонах частот 2,4 ГГц і 5 ГГц. Точка доступу DWL-6620APS може працювати як в автономному режимі, так і під управлінням уніфікованих бездротових контролерів D-Link.

Підтримувані стандарти: 802.11a; 802.11b; 802.11g; 802.11n; 802.11ac.

Розширені функції: IEEE 802.11k, IEEE 802.11r, Auto Channel selection, Auto Channel selection, MU-MIMO, Wireless Multimedia (WMM), Wireless Distribution System (WDS), Band Steering, Airtime Fairness.

Безпека бездротового з'єднання: WPA/WPA2-Personal/Enterprise, AES и TKIP, виявлення несанкціонованих точок доступу, фільтрація за MAC-адресами.

Швидкість бездротового з’єднання: у діапазоні 2,4 ГГц – до 400 Мбіт/с; 5 ГГц – 867 Мбіт/с.

Рисунок 3.5 – Бездротова точка доступу D-Link DWL-6620APS

Із характеристик видно, що дана модель задовольняє всім вимогам. Є підтримка стандарту 802.11r, одночасна робота в двох діапазонах, забезпечення високою пропускною здатністю та підтримка стандарту 802.11n, вона є уніфікована з контролером D-Link DWC-1000 . Також, окрім того, що DWL-6620APS відповідає критеріям вибору, вона має ще ряд деяких переваг. За допомогою технології MU-MIMO є можливість одночасно передавати незалежні потоки даних кільком клієнтам через різні антени. Це дозволяє більш ефективно використовувати радіоканал для передачі даних і значно збільшує загальну пропускну здатність мережі. DWL-6620APS

підтримує технологію 2x2 MU-MIMO, забезпечуючи максимальну продуктивність бездротової мережі. Підтримка стандарту 802.1p Quality of Service (QoS) для збільшення пропускної спроможності та продуктивності при передачі чутливого до затримок трафіку, наприклад, VoIP або потокового відео. Бездротова точка доступу DWL-6620APS також підтримує WMM, таким чином, в разі перевантаження мережі, пріоритет отримає чутливий до часу трафік. Підтримка технології Band Steering дозволяє бездротової точці доступу DWL-6620APS виділити клієнту оптимальний діапазон щоб уникнути перевантаження мереж і забезпечує, таким чином, плавну передачу потокового відео і швидке завантаження сторінок з мобільних пристроїв. Завдяки технології Airtime Fairness виконується рівномірний розподіл часу передачі, таким чином, в разі перевантаження мережі чутливий до часу трафік може бути переданий до кожного клієнта, що забезпечує високу продуктивність навіть при підключенні пристроїв попередніх версій. Підтримка PoE (Power over Ethernet) – дозволяє передавати дані і живлення по одному Ethernet-кабелю, що значно полегшує завдання встановлення.

4 ПРОЕКТУВАННЯ МЕРЕЖІ В OPNET MODELER®

4.1 Обґрунтування вибору імітаційної програми OPNET Modeler®

Щоб впевнитись, що мережа здатна забезпечити необхідну пропускну здатність, після отриманих розрахункових результатів необхідно провести моделювання роботи всієї мережі і потім порівняти дані розрахунків та моделювання.

Моделювання в програмному пакеті OPNET Modeler® – це дискретно-подієва симуляція (DES). Симуляція в OPNET Modeler® підрозділяється на три структури, а саме: модель мережі, модель вузла, і модель процесу. Як правило, симулятор містить в собі величезну бібліотеку попередньо визначених моделей для різних симуляцій і дозволяє користувачам визначати, призначені для користувача, моделі. Функція графічного інтерфейсу користувача в пакеті OPNET Modeler® допомагає створити загальне середовище, яке називають проектом. На основі цього проекту користувач може розробити кілька сценаріїв мережі для того, щоб оцінити і проаналізувати продуктивність цієї мережі в різних обставинах. Також, це програмне забезпечення може бути використано для великого ряду задач, наприклад, типові створення і перевірка протоколу зв'язку, аналіз взаємодій протоколу, оптимізація та планування мережі. також можливо здійснити за допомогою пакета перевірку правильності аналітичних моделей, і опис протоколів.

Програмний пакет OPNET Modeler® надає чотири редактора для розробки уявлення модельованої системи. Ці редактори – Мережа, Вузол, Процес і Редактори параметрів – організовані ієрархічно, як показано на рисунку 4.1. Кожен рівень ієрархії описує різні аспекти повної моделі моделювання. Моделі, розроблені на одному рівні ієрархії, використовуються моделями на наступному вищому рівні. Це призводить до створення дуже

гнучкого середовища моделювання, в якій загальні моделі можуть бути розроблені і використані в багатьох різних сценаріях.

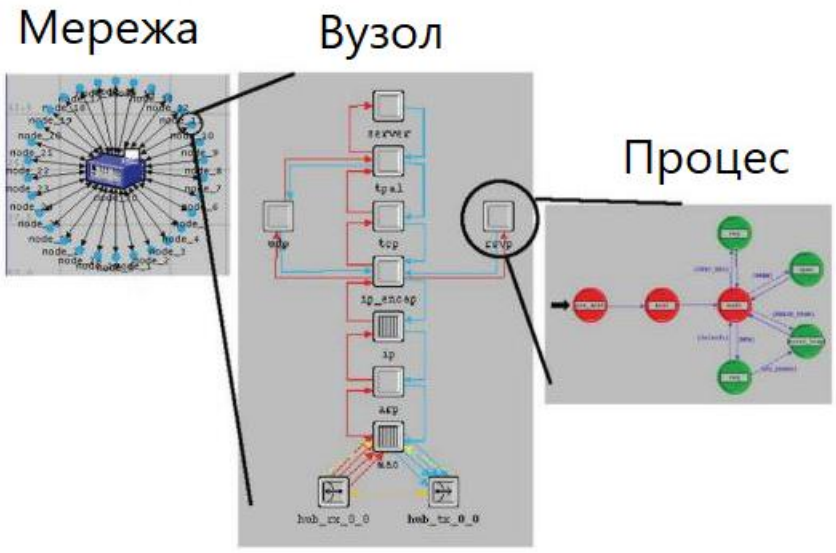

Рисунок 4.1 – Графічні редактори програмного пакету OPNET Modeler®

Головними перевагами програмного пакету OPNET Modeler® є:

– пакет OPNET Modeler® можна використовувати для моделювання всієї мережі, включаючи маршрутизатори, комутатори, протоколи, сервери і окремі додатки, які вони підтримують. Можлива підтримка великого діапазону комунікаційних систем від однієї локальної мережі до глобальних мереж;

– дискретно-подієвий алгоритм програм OPNET Modeler® для моделювання мереж є найшвидшим і комерційно доступним рішенням. Зазвичай потрібно всього кілька хвилин для завершення моделювання більшості лабораторних експериментів.

Отже, в кінці можна додати, що OPNET за своєю суттю має три основні функції: моделювання, симуляція і аналіз. Для симуляції надає інтуїтивно зрозуміле графічне середовище для створення всіх видів моделей протоколів. Для симуляції він використовує 3 різні передові технології і

може застосовуватися для вирішення широкого кола завдань. Для аналізу результати моделювання і дані можуть бути проаналізовані і відображені дуже просто. Зручні графіки, діаграми, статистика і навіть анімація можуть бути створені в OPNET для зручності користувачів. Тому саме OPNET Modeler® буде використовуватись в подальшому моделюванні.

4.2 Проектування мережі в OPNET Modeler®

В програмі OPNET Modeler® буде проводитись моделювання третього поверху. Поставленою метою є отримання графіків, на яких буде показана пропускна здатність мережі.

Надалі моделювання буде проходити за двома сценаріями. В першому сценарію буде показано функціювання мережі під час проведення аудиторних занять, тобто коли майже всі користувачі знаходиться в предметних аудиторіях. У другому сценарію буде симульована робота мережі під час перерви, тобто коли основна кількість користувачів знаходиться в коридорах, викладацьких або за межами навчального корпусу.

На першому етапі створення проекту необхідно дати назву проєкту, вибирається розмір мережі (world, enterprise, campus, office). Для цієї роботи було вибрано розмір – office. Необхідно вибрати конкретні розміри місцевості (м), на якій буде розташовуватися мережу. Для створюваної мережі встановимо розміри 53×23 метрів, саме такий розмір третього поверху. Також, додано план поверху для наочності.

Надалі відбувається проектування першого сценарію.

Найперше це вибір компонентів, які необхідні для проекту. Модель мережі створюється за допомогою редактора з використанням вузлів (nodes) і каналів зв'язку (links) з бази ресурсів (вікно з зображеннями вузлів і зв'язків, Object Palette). У таблиці 4.1 показані необхідні компоненти для мережі.

Таблиця 4.1 – Компоненти мережі

Кіл.	Компоненти	База ресурсів	Опис
170	wlan_wkstn (Mobile node)	wireless_lan	Комп'ютери (мобільний вузол)
1	ethernet_server	internet_toolbox	Сервер
1	ethernet16_switch_adv	internet_toolbox	Комутатор
1	ethernet4_slip8_gtwy_adv	internet_toolbox	Маршрутизатор
7	wlan_ethernet_router	wireless_lan	Точка доступу
2	eth_switched_lan_adv	lan	LAN
11	100BaseT	internet_toolbox	з'єднувальні лінії
1	Application Config	wireless_lan	Application Config визначає стандартні і призначені для користувача додатки, використовувані в імітаційному моделюванні, включаючи параметри трафіку і якості обслуговування
1	Profile Config	wireless_lan	Profile Config визначає режими використання додатків користувачем або групою користувачів

Для настройки обладнання необхідно натиснути правою кнопкою миші на цьому обладнанні і вибрати в меню пункт Edit Attributes. Залежно від вибраного обладнання в робочій області з'явиться вікно з різним набором параметрів, що настроюються.

Налаштування точок доступу відбувається шляхом вибору стандарту за яким вона буде працювати. Було вибрано стандарт 802.11n, а також підтримку стандарту 802.11r. Інші параметри були залишені по замовчуванню. Нижче наведена таблиця 4.2 параметрів моделювання точки доступу. Також необхідно додати, що ТД взаємодіють з абонентами відповідно до розрахунків і рекомендацій зазначених в главі 3. В таблиці 4.3 показано скільки користувачів підключається до кожної точки доступу.

Таблиця 4.2 – Параметри моделювання точки доступу

Фізичні характеристики	802.11n
Швидкість передачі даних	600 Мбіт/с
Можливість роумінгу	Включено

Таблиця 4.3 – Кількість підключених абонентів до ТД

Точка доступу	Кількість абонентів
TD1	20
TD2	20
TD3	18
TD4	17
TD5	17
TD6	20
TD7	20

Налаштування параметрів програми та профілю. Тип трафіку задається за допомогою елемента палітри Application Definition. Application Definition містить характеристики додатків, створюваних у вигляді потоків і мають власні параметри трафіку. Було створено 4 стандартних потоки такі

як: http, video conferencing, chat, email. Тип трафіку вибирався відповідно до того, який найбільше використовується на території університету. В таблиці 4.4 наведені параметри налаштування Application Definition.

Таблиця 4.4 – Налаштування Application Definition

Визначення додатків	http, video conferencing, chat, email

Після створення потоків додатків необхідно конфігурувати профілі користувачів, які працюють в спроектованої мережі. цю функцію виконує елемент палітри Profile Definition.

Кожному профілю дається назва і описується ряд користувальницьких характеристик: час початку роботи, тривалість, закінчення, інтенсивність його перебування і роботи в мережі і якими із запропонованих (створених) додатків він користується. Всі параметри встановлені по замовчуванню, окрім параметру використання додатків. Таким чином, було задано, що користувач використовує всі типи трафіку, які були задані в Application Definition. В таблиці 4.5 наведені параметри налаштування Profile Definition.

Таблиця 4.5 – Profile Definition

Ім’я профілю	all
Використовувані додатки профілю	http, video conferencing, chat, email

Під час налаштування сервера потрібно прописати тип трафіку, що генерується користувачами. Найпоширеніші типи трафіку: дані, мова, відео. Кожен з них пред'являє різні вимоги до передачі, забезпечення необхідної якості обслуговування, виділенню достатньої пропускної здібності. В параметрі Supported Profiles було вибрано підтримку всіх додатків, які використовуються користувачами. В параметрі Supported Service було

вибрано підтримку всіх сервісів (All Services). В таблиці 4.6 наведені параметри налаштування сервера.

Таблиця 4.6 – Налаштування серверу

Додатки: Підтримувані профілі	all
Додатки: Підтримувані сервіси	Всі сервіси

Як правило, додаткове налаштування комутатора не потрібне, якщо немає необхідності реконфігурації портів або настройки VLAN.

Оскільки необхідно враховувати дротові локальні мережі, то було додано локальну мережу в дві аудиторії. При налаштуванні було вибрано для першої аудиторії 28 робочих станцій, для другої – 12.

При налаштуванні кінцевих пристроїв абонентського доступу було задано такі параметри: підтримуваний стандарт – 802.11n, підтримка стандарту 802.11r та підтримувані додатки всі, які були задані в Application Definition. В таблиці 4.7 наведені параметри налаштування кінцевих пристроїв.

Таблиця 4.7 – Налаштування кінцевих пристроїв абонентського доступу

Додатки: Підтримувані профілі	all
Додатки: Підтримувані сервіси	Всі сервіси
Можливість роумінгу	Включено

На рисунку 4.2 показано модель функціювання схеми для першого сценарію.

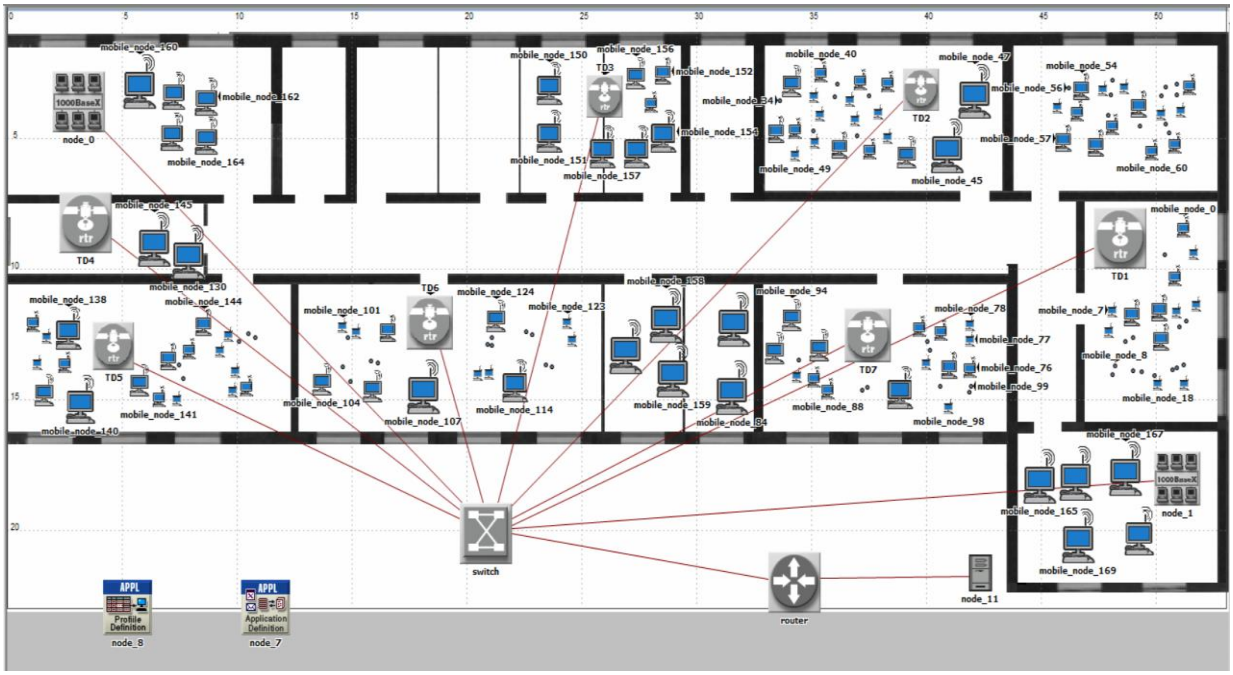

Рисунок 4.2 – Модель функціювання схеми для першого сценарію

Як вже зазначалось раніше другий сценарій описує перерву в аудиторних заняттях. Для цього сценарію налаштування пристроїв залишилося незмінним. Тут змінилися лише кількість та розташування користувачів. В першому сценарії їх було 170, тому що в першому сценарію показано навчальний процес, коли всі студенти та викладачі знаходяться в аудиторіях, а деяка кількість користувачів в інших приміщеннях (кафедра, викладацька). В другому 120 користувачів перебувають в більшій кількості в коридорах та інших не аудиторних приміщеннях, деякі користувачі залишили поверх. Також, в комп’ютерних класах кількість використовуваних комп’ютерів в першому сценарії було 20, в другому – 1, вважається що під час перерви користувачі залишають комп'ютерні класи або там залишається мінімальна кількість людей. На рисунку 4.4 показано модель функціювання схеми для другого сценарію.

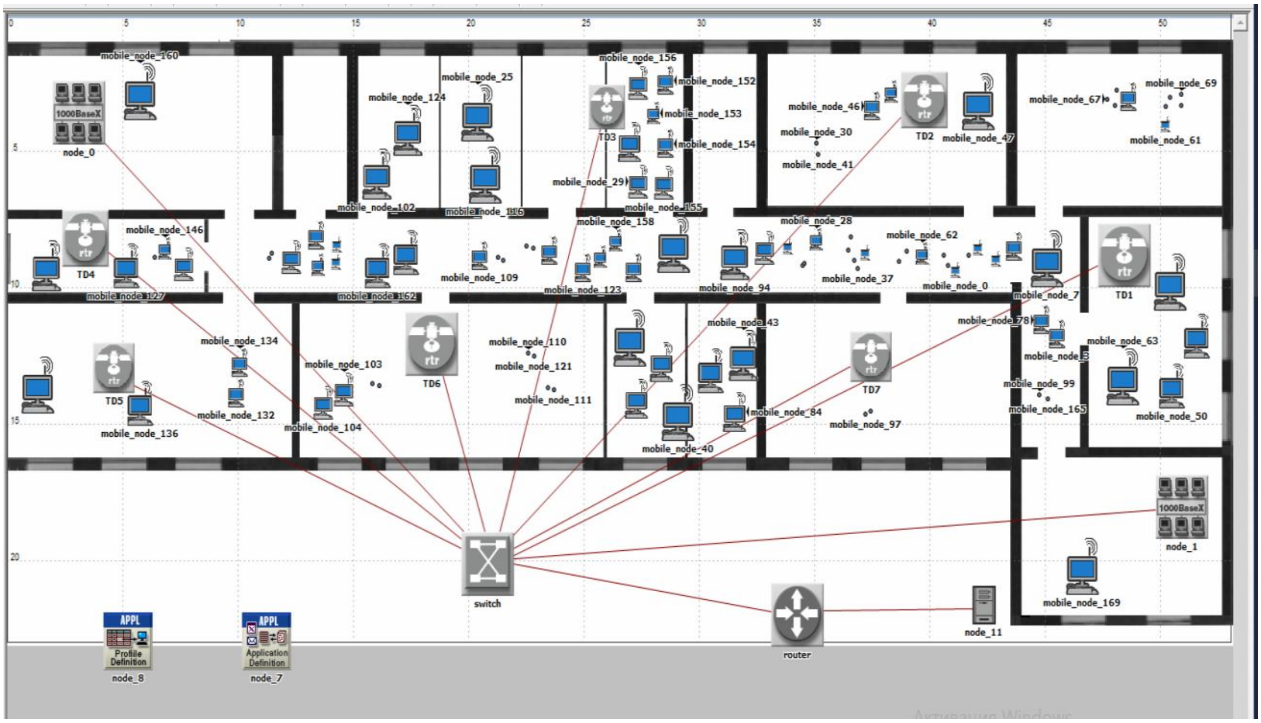

Рисунок 4.4 – Модель функціювання схеми для другого сценарію

4.3 Симуляція в пакеті OPNET Modeler® та порівняння отриманих результатів

Після того, як зроблено внесення всіх елементів мережі, треба вибрати тип необхідних статистик. Перед початком процесу симуляції необхідно налаштувати деякі параметри симуляції. Для цього на панелі інструментів потрібно натиснути кнопку configure/run simulation і увійти в режим симуляції. Пакет OPNET Modeler® пропонує вказати тривалість роботи мережі (в даному випадку – 80 хв.). У наступних закладках є можливість налаштування глобальних параметрів мережі, параметрів моделювання для кожного елемента, виведення звітів, анімації під час моделювання та ін. Наступним кроком є запуск симуляції, шляхом натискання кнопки Run. Якщо під час моделювання мережі не було зроблено помилок, то симуляція буде успішною і надалі буде можливим переглядати необхідні результати.

Для сценарію 1 на рисунку 4.5 наведені отримані результати для сценарію.

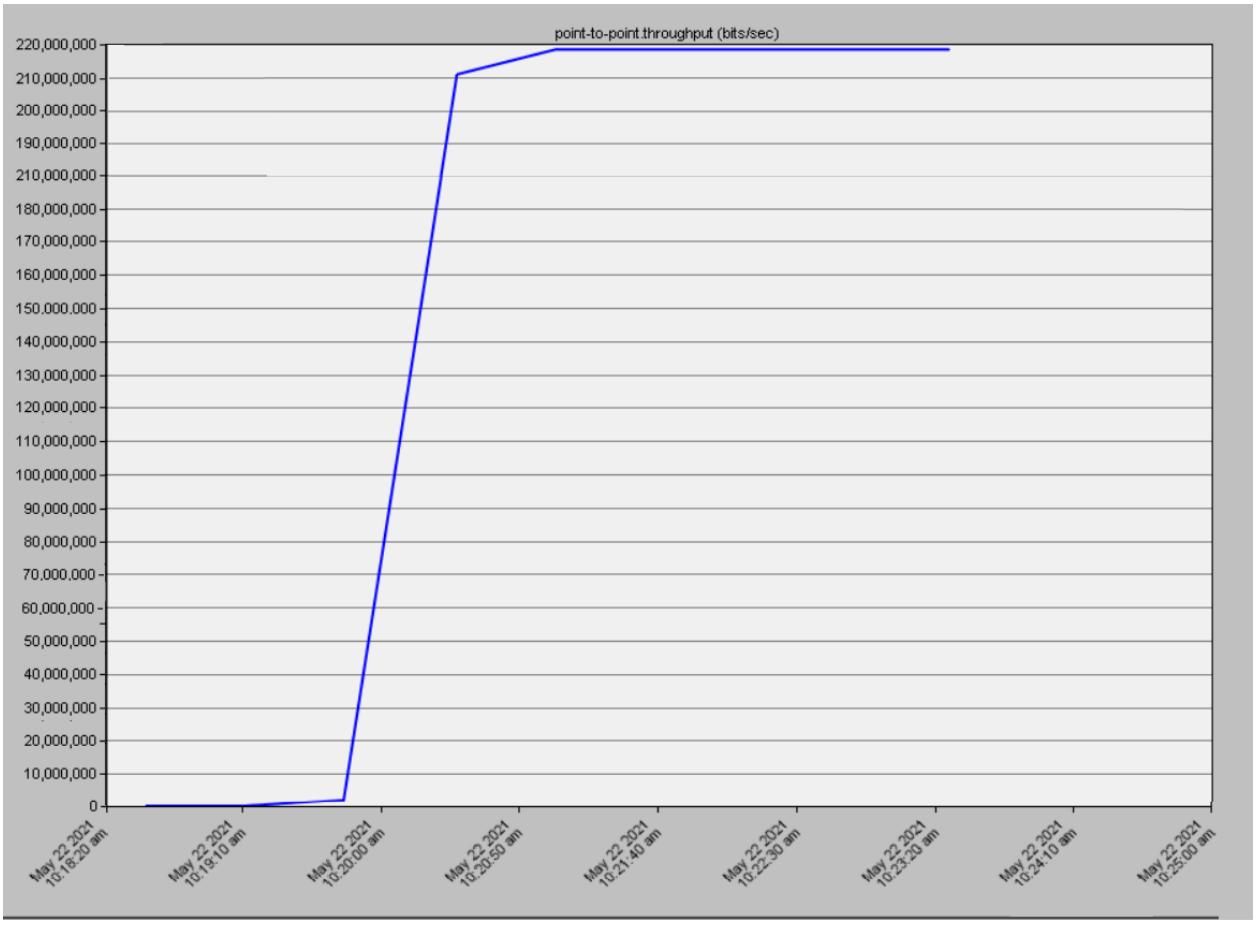

Рисунок 4.5 – Результати симуляції для сценарію 1

Із пункту 3.2 було розраховано, що необхідна пропускна здатність дорівнює 150 Мбіт/с. Із рисунку 4.5 видно, що пропускна здатність дорівнює 220 Мбіт/с. Така різниця викликана тим, що розрахунок необхідної пропускною здатності мережі проводився тільки для бездротових пристроїв, і не було взято до уваги дротові локальні мережі. Отже, можна вважати, що симуляція в OPNET Modeler® показала цілком достовірні результати.

Для другого сценарію були зроблені такі ж кроки, як і для першого. Різниця полягає в тому, що тривалість симуляції було вибрано 30 хв. (тривалість великої перерви).

Результати сценарію 2 представлені на рисунку 4.6.

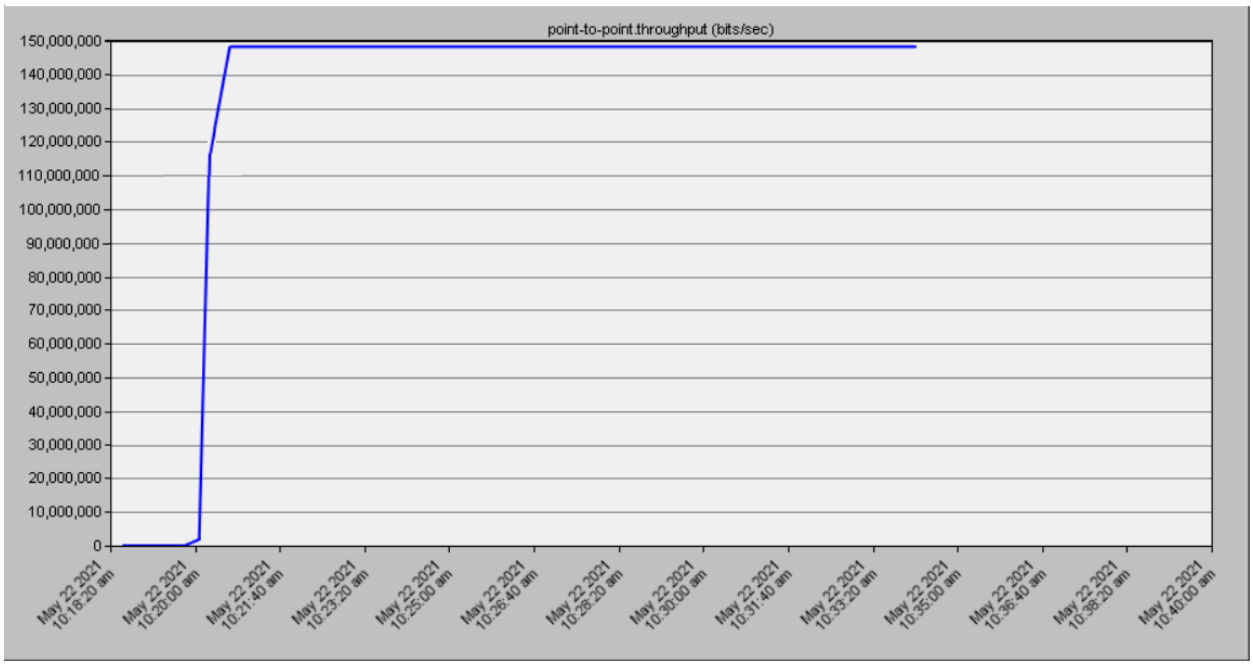

Рисунок 4.6 – Результати симуляції для сценарію 2

Із рисунка видно, що при зменшенні кількості користувачів, пропускна здатність дорівнює 150 Мб/с.

Створивши моделі функціювання схем, вдалось провести симуляцію та отримати значення пропускної здатності.

Із графіків видно, що значення пропускної здатності відповідають розрахунковим.

Таким чином, було обґрунтовано вибір імітаційної програми OPNET Modeler® , показані основні переваги цієї програми. Далі для побудови схеми функціонування був проведен вибір обладнання та налаштування відповідно до параметрів проектованої мережі. Після цього було вибрано тип статистик та запущено симуляцію в програмі спочатку для першого, потім для другого сценаріїв. За загальним рахунком результати відповідали розрахунковим.

Отже, проєктована мережа здатна працювати в реальних умовах.

ВИСНОВКИ

В ході дипломного проектування було запропоновано рішення що допоможе поліпшити організацію навчального і наукового процесів та ефективність управлінської діяльності в університеті шляхом модернізації та розширення мережі доступу до інформаційних ресурсів третього корпусу. Досягнення поставленої мети можливо отримати за рахунок об’єднання і перерозміщення існуючих та нових точок доступу Wi-Fi.

Для цього в роботі були визначені основні вимоги до оновленої мережі та необхідний стандарт технології 802.11. Також було проведено дослідження кількості користувачів на поверхах навчального корпусу та проведені необхідні розрахунки. На підставі теоретичних розрахунків в програмі D-Link Wi-Fi Planner Pro вдалось здійснити планування місць розташування точок доступу Wi-Fi з урахуванням місцевості. В результаті цього була отримана модель схеми оптимального розміщення точок доступу на третьому поверсі навчального корпусу, що в свою чергу стало підґрунтям для вибору необхідного обладнання.

З метою переконання, що обране обладнання відповідає вимогам до мережі, що модернізується, була розроблена імітаційна модель в програмному пакеті OPNET Modeler® та проведено порівняння розрахункової пропускної здатності із змодельованою в програмі. Таким чином було підтверджено правильність вибору.

Треба зазначити, що QoS мережі, яка пропонується буде ефективною, лише якщо узгоджені параметри QoS у всій мережі університету. Будь-яка частина шляху, яка не підтримує пріоритети QoS, може привести до погіршення якості. Це включає застосування параметрів на всіх пристроях користувачів, мережевих перемикачах, маршрутизаторах та проксі-серверів до Інтернету.

ПЕРЕЛІК ПОСИЛАНЬ

1. Віртуальне навчальне середовище Moodle [Електронний ресурс]: Режим доступу: https://ru.wikipedia.org/wiki/Moodle .

2. Кількість використовуваного трафіку додатками [Електронний ресурс]: Режим доступу: https://teztele.com/skolko-internet-trafika-potreblyayut-populyarnye-prilozheniya/ .

3. Використовуваний трафік Zoom [Електронний ресурс]: Режим доступу: https://zoomapp.ru/faq/how-much-data-does-zoom-use .

4. Технологія ZigBee [Електронний ресурс]: Режим доступу: https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/ .

5. Григорьев В.А. Системы и сети радиодоступа [Текст] / В.А. Григорьев О.И. Лагутенко, Ю.А. Распаев. – Москва: Видавничо-поліграфічний центр “ЭкоТрендз”, 2005г – 373 с.

6. Безпека в бездротовій технології ZigBee [Електронний ресурс]: Режим доступу: http://www.rovdo.com/zigbee-security .

7. Przemysław Machan Comparison of the IEEE 802.11, 802.15.1, 802.15.4 and 802.15.6 wireless standards [Text] / Przemysław Machan, Jan Magne Tjensvold Norwood: ARTECH HOUSE, 2007 – 7 p.

8. Технологія Bluetooth [Електронний ресурс]: Режим доступу: http://1234g.ru/blog-of-wireless-technologies/about-bluetooth/chto-takoe-bluetooth-i-kak-on-rabotaet .

9. Рашич А.В. Сети беспроводного доступа WiMax [Текст] / А.В. Рашич. – Санкт-Петербург: Видавництво політехнічного університету, 2011г – 179 с.

10. Роумінг в стандарті 802.11i [Електронний ресурс]: Режим доступу: https://www.networkworld.com/article/2324422/vendors-innovate-beyond-802-11i-roaming-standards.html .

11. Przemysław Machan On the fast BSS transition algorithms in the IEEE 802.11r local area wireless networks [Text] / Przemysław Machan, Jozef Wozniak Norwood: ARTECH HOUSE, 2011 – 8 p.

12. Bien Van Quang A Survey on Handoffs – Lessons for 60 GHz Based Wireless Systems [Text] / Bien Van Quang, R. Venkatesha Prasad, Ignas Niemegeers, 2011 – 23 p

13. 802.11r or Fast Transition (FT) for fast secure Roaming

14. Сценарии проектирования и развертывания сети стандарта Wi-Fi [Електронний ресурс]: Режим доступу: https://komway.ru/texnologii/wi-fi/wi-fi-2 .

15. Планировщик беспроводных сетей [Електронний ресурс]: Режим доступу: https://tools.dlink.com/wifiplanner .