Державний університет «Одеська політехніка»

Інститут штучного інтелекту та робототехніки

Кафедра комп’ютерних систем

Пояснювальна записка

до дипломної роботи магістра

на тему: «Дослідження методів покращення ефективності комп’ютерної мережі міської інфраструктури»

Виконав студент 2 курсу групи УК-162

спеціальності «Спеціалізовані комп’ютерні системи»

Кривоконь Артем Сергійович

Керівник: Стрельцов О.В.

Рецензент: _____

Одеса 2021

ЗМІСТ

ВСТУП

Сучасні тенденції по розвитку передових технологій рішуче змінюють загальне положення по створенню нових проектів та ідей. Головною метою будь-якої технології є поліпшення умов життя людства, як побутових, так і промислових, корпоративних, соціальних тощо. Концепція «розумного міста» втілює собою всі амбіції та побажання на десятки, якщо не сотні років технічного прогресу вперед. Поширення даної технології у маси не змушує себе чекати. Якщо зацікавитися у поліпшенні свого особистого життя шляхом впровадження відповідних девайсів, то ви так чи інакше стаєте частиною майбутнього розумного міста. Можна почати з розумного фітнес браслету, який буде відстежувати вашу фізичну активність впродовж дня, а завершити в будинку, де в кожному куті буде знаходитися щось «розумне». Амбіції амбіціями, але проект мусить створюватися інженерами, а не маркетологами, і саме для них в першу чергу важливий аспект керування майбутнім проектом, щоб користування і його подальше впровадження в буденність були незаперечними и безперешкодними.

Повсюдне впровадження розумних технологій будує з них комп’ютерну мережу, яка потребує керування собою, вирішення виникаючих проблем та безперервну модернізацію. За необмеженою кількістю ідей виникла велика кількість як різних, так і однакових концепцій, але кожна з них має унікальні риси, які так чи інакше впливають на процес підтримки її працездатності.

Актуальність даної роботи полягає у відсутності єдиного рішення стосовно управління комп’ютерною мережею, адже кожна мережа будується на власний лад і методи її управління виникають тільки після її втілення. Даний проект створений для узагальнення основних положень, стосовно управління мережею.

Мета роботи полягає в удосконаленні задачі по управлінню комп’ютерною мережею.

Для досягнення даної мети необхідно:

- Проаналізувати сучасне становище концепції «розумного» міста;
- Побудувати гібридний метод управління комп'ютерною мережею;
- Моделювання запропонованої мережі;

Об'єкт дослідження – процес управління мережею міської інфраструктури.

Предметом дослідження є методи управління комп'ютерною мережею, за рахунок покращення рівню управління комп'ютерною мережею міської інфраструктури без втручання в особистий простір користувача та максимально можливий контроль за працездатністю та відмовостійкістю.

Інноваційне рішення полягає у створенні універсального підходу до керування комп'ютерною мережею як нових проектів, так і впровадження у вже існуючі. Дана робота будується на аналізі існуючих моделей керування, їх доопрацювання та впровадження запропонованої ідеї.

Практичне значення одержаних результатів полягає в можливості втілення в будь-якій мережі в якості універсального технічного рішення та покращенню показників продуктивності, таких як кількість затраченого часу на усунення причини відмови та спрощення процесів проектування, моделювання, розгортання та підтримку нової мережі. Проект вирішує важливі питання по управлінню комп'ютерною мережею в практиках, де певні операції не вважаються необхідними.

Кваліфікаційна робота створена для випробовування запропонованого підходу до ефективного керування комп'ютерною мережею. Результати роботи не були апробовані на реальних проектах. Висновки роботи та отримані результати перебувають на етапі теорії та підлягають дослідженню ефективності в участі існуючих проектів як тестовий варіант.

1. АНАЛІТИЧНИЙ ОГЛЯД

1.1 Опис і постанова загальної проблеми

Розглянута в даній роботі концепція розумного міста не має чіткого єдиного рішення. Саме тому, на створення та реалізацію методу керування комп'ютерною мережею, необхідно створити власний варіант, який задовольняє усі мінімальні потреби у працездатності майбутнього проекту, до якого можна створити чітку послідовність дій та маніпуляцій по її керуванню.

За допомогою аналізу існуючих рішень та впровадженню запропонованих ідей, буде досягнута єдина концепція-вказівник для початку роботи по керуванню комп'ютерною мережею.

Через велику кількість різних варіацій комп'ютерних мереж, відсутність концептуального рішення по вирішенню рядових проблем по їх працездатності, до керування комп'ютерною мережею справа доходить постфактум після її створення та впровадження в реальний проект. Дана робота покликана впровадити вирішення проблеми керування на етапі створення самої мережі.

Слід виділити основні етапи майбутньої роботи:

- Аналіз існуючих рішень, огляд їх переваг та недоліків
- Опрацювання отриманої інформації та її співставлення з потребами майбутніх проектів
- Виділення недоліків та переваг описаної концепції
- Формування основних положень по створенню методу керування комп'ютерною мережею
- Опис отриманого результату на прикладі моделювання тестової мережі

1.2 Аналіз існуючих рішень та джерел інформації

Побудова сучасних комп’ютерних мереж, чи то локального типу, чи міського, будується, перш за все, з метою покращення вже існуючого функціоналу, а надалі, додавання нових функцій, вирішення старих проблем шляхом усунення проблемного вузла або переосмислення методів по його запровадженню. Дані методи використовуються все рідше і рідше, проте досі деякі вважають, що усунення предмета проблеми вирішить і саму проблему.

Даний варіант не підходить під сучасні реалії і не має майбутнього. Саме тому для вирішення проблеми іншим шляхом інженери шукають різний підхід до побудови самої мережі на етапі проектування, щоб заздалегідь уникнути таких ситуацій.

Сучасні тренди по побудові комп’ютерних мереж концепції «розумного міста», передбачають неможливість усунення певних деталей та нюансів майбутнього проекту, тому необхідно вирішувати таким чином, щоб уникнути можливих проблем ще до втілення самої ідеї в життя. У цьому допомагають засоби моделювання, теоретична основа та практичне втілення невеликих вузлів для отримання наочного результату. Надалі розглянемо саму концепцію «розумного міста», шляхи її впровадження та модернізації, а також існуючі моделі керування комп’ютерними мережами, їх переваги та недоліки.

Основні ідеї концепції комп’ютерної мережі «розумне місто»

Загальний темп розвитку стрімко росте з плином часу. Сучасні технології є прямими вихідцями так званої четвертої індустріальної революції. Саме вона подарувала світу глобальні промислові мережі, інтернет речей, нейромережі, штучний інтелект, розподілений простір, мережевий колективний доступ та багато чого іншого.

Розвиток інтернету, інфокомунікаційних технологій, стійких каналів зв’язку, хмарних технологій та цифрових платформ, а також інформаційний «вибух» виплеснувшихся з різних каналів даних, забезпечили появу відкритих інформаційних систем та глобальних промислових мереж, що виходять за кордони окремого підприємства та взаємодіючих між собою.

Основними компонентами індустрії 4.0 в плані телекомунікацій та інтернету вважаються:

- Автономні роботи
- Моделювання
- Інтеграційна система
- Інтернет речей
- Кібербезпека
- Хмарні обчислення
- Адитивна промисловість
- Доповнена реальність
- Big Data

Багато з цих елементів вже давно і більш ніж успішно реалізовані та використовуються на практиці, але саме їх об’єднання в одну цілісну систему дозволить розвинути концепцію «Індустрії 4.0» та забезпечити новий рівень ефективності підприємства та додаткових прибуток за рахунок використання цифрових технологій [1].

Постанова задачі по створенню комп’ютерної мережі міського типу, яка оснащена тисячами датчиків та мікроконтролерів, які спілкуються між собою в режимі реального часу виникла з бажання створити собі комфортне життя та отримала глобальне світове охоплення. Загальний вигляд концепції, без урахування виняткових особливостей, присутніх кожному місту, зображений на рисунку 1.1:

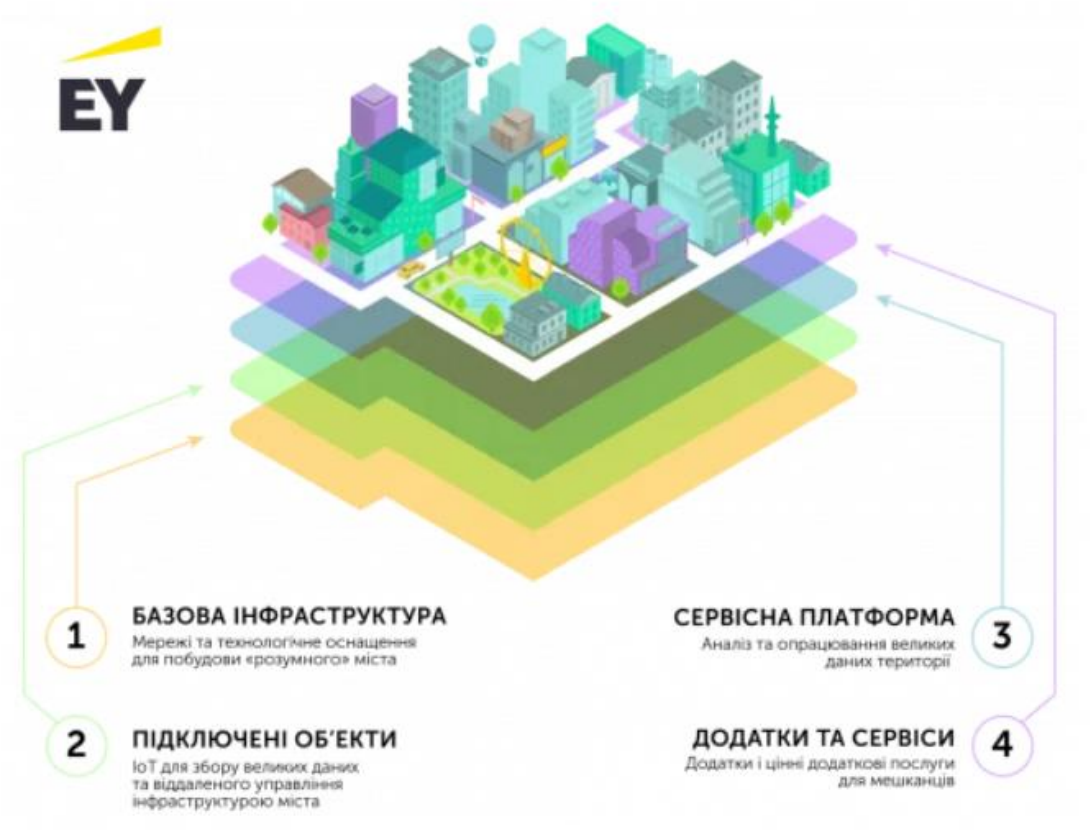

Рисунок 1.1 – загальна концепція розумного міста з точки зору комп'ютерних мереж та телекомунікацій [2]

Використання приладів розумного будинку є буденністю, тому необхідно передбачити декілька шляхів розвитку у створення мережі, щоб була можливість підлаштуватися під різні прилади від різних виробників з можливістю масштабування мережі. Необхідно пам'ятати, що перш за все, метою стоїть створення комфортних умов для життя, тому не слід втручатися до особистої інформації та як слід потурбуватися про інформаційну безпеку майбутньої комп'ютерної мережі. Будь-яка вразливість є потенційною загрозою, адже втрата персональної інформації, навіть не настільки важливої як час виходу з дому, або час, коли користувач йде до ліжка, може обернутися пограбуванням.

Для дослідження методів керування комп'ютерними мережами, перш за все необхідно розглянути, перш за все, саму технологію побудови мережі, її варіації та основні положення. В концепції «розумного міста» розглядається мережа одного

розумного будинку як мінімальна структурна одиниця. Як і у будь-якого проекту, він має очевидні переваги, інакше не мав би необхідності у існуванні.

Основні переваги, які виділяє автор:

- Очевидна економія часу. Час, витрачений на щоденну побутову роботу стає вільним, адже примітивні побутові задачі виконують пристрої, якими можна керувати.
- Гарний спосіб впровадження в повсякденне життя новітніх технологіями. Використання нових пристроїв з різним функціоналом змушує корпорації підлаштовуватись під конкуренцію і вигадувати, чим здивувати рядового користувача.
- Вирішення проблеми масштабування. Побудова мережі в даному проекті буде будуватись на розподіл всієї мережи на частини ієрархічним способом. Замість однієї великої цільної мережі, отримуємо розбиту на підмережеві складові систему, якими легко керувати и сфокусуватись лише на певних аспектах чи ділянках всієї мережі.

Переваги стрімкого розвитку розумних міст, зміни в житті людей та кількісні показники зображені на рисунку 1.2:

Рисунок 1.2 – основні постулати та переваги розумних міст [3]

Основні функції, представлені у класичному прикладі розумного будинку [4]:

- Функція охорони. Дана функція включає в себе: охорону від проникнення в якості, наприклад, сигналізації; імітація присутності – за довгої відсутності господаря, будинок може сам увімкнути світло, музику; контроль периметру та відеоспостереження – за допомогою датчиків та камер відеоспостереження можливий безперервний контроль за периметром власного будинку; тривожна кнопка на випадок необхідності у екстреній допомозі.
- Функція безпеки. В разі протікання води, система здатна моментально сповістити про це господаря та примусово блокувати водопостачання. Запобігання витоку газу в разі несправності газопостачальної труби шляхом перекриття газової магістралі та примусовому провітрюванні

приміщення (що є частиною протипожежної безпеки, яка також присутня).

- Комфорт. Керування температурою в кожній з кімнат, детальне регулювання рівня яскравості світла та спеціальні сценарії освітлення за таймером чи орієнтовно по годиннику.
- Сервіс. Зміна та корекція існуючих параметрів та сценаріїв у будинку за допомогою комп'ютеру, смартфону чи планшету. GSM-моніторинг дозволяє підтримувати віддалене інформування про події у будинку через смартфон або планшет.

Згідно закордонної статистики, технологія розумного будинку дозволяє заощаджувати на: експлуатаційних витратах – до 30%; оплаті за воду та водопостачання – до 41%; електроенергії – до 30%; опаленні – до 50% [4].

Виникла проблема перенаселеності міст тягне за собою очевидну проблему вирішення комфортного сумісного проживання населення міст. Проекти концепції «розумне місто» є оптимальним рішенням та єдиним засобом керування інфраструктурою.

За прогнозами до 2040 року 60% населення буде жити в містах [5]. На сьогоднішній день, 80% населення США мешкає в містах та мегаполісах, проти 60% лише 50 років тому. За прогнозами IDC, до 2021 року глобальні витрати на розумні міські ініціативи зростуть до $ 135 мільярдів. В 2017 році у США було 29 мільйонів будинків, які використовували розумні технології для дому. За оцінками консалтингової компанії McKinsey, щороку їх кількість зростає на 31%.

Завдяки популяризації розумних технологій, стрімкого їх впровадження у буденне життя як населення, так і всього міста в цілому, а також урбанізації, влада прагне якомога краще забезпечити поточний темп розвитку та підвищити ефективність вже існуючих рішень, задля створення добробуту громадян. Рішення розповсюджуються на всі сфери діяльності людини: від буденного паркування

автомобіля, до створення прозорого уряду самоврядування, підвищуючи довіру населення до влади. Робиться це шляхом створення спеціальних додатків, розміщенню розумних пристроїв, роботою з великими даними (Big Data). Інфографіка розвитку попиту на «розумні» технології зображена на рисунку 1.3:

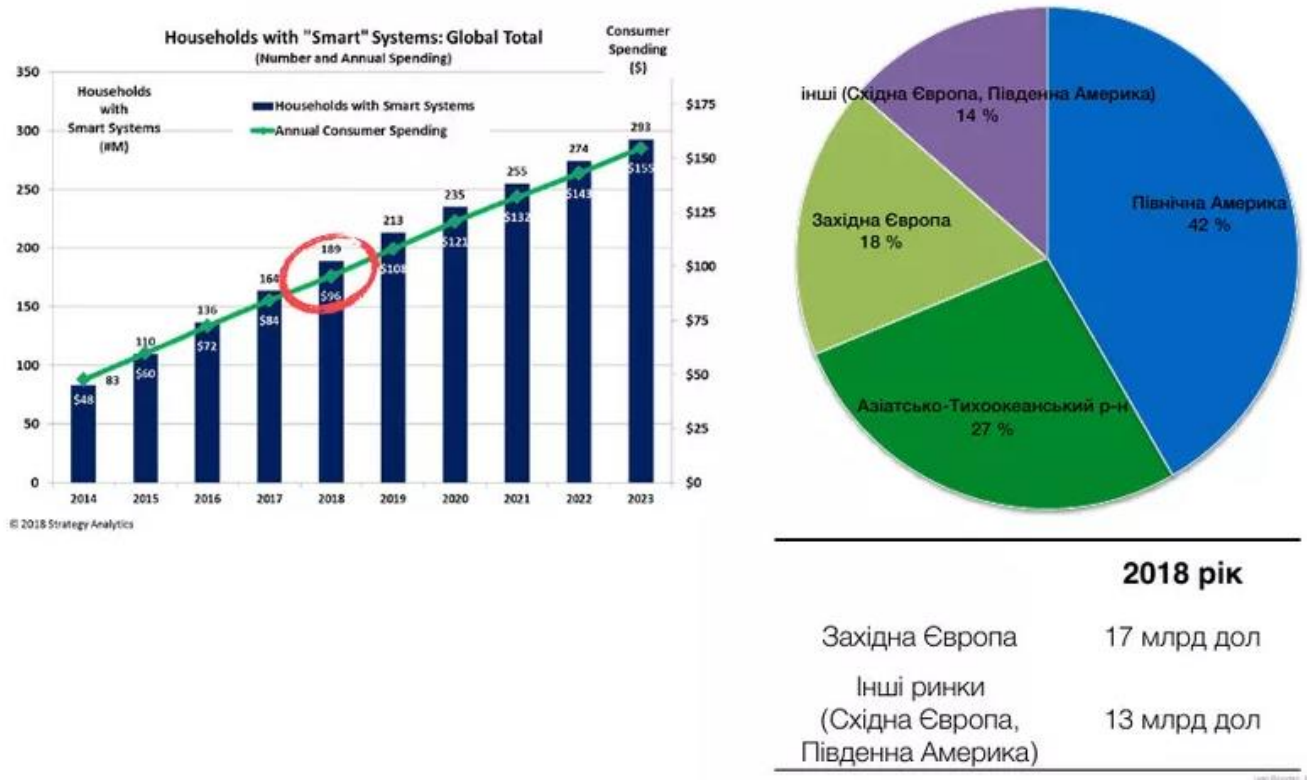

Рисунок 1.3 – розвиток та популярність технології «розумних будинків» на світовому ринку за даними 2018 року [6]

Фахівці виділяють 4 напрямки розвитку розумного міста: мобільність – мобільність міського транспорту (включаючи громадський, персональний та немоторизований); охорона здоров'я – її якість, доступ громадян до медичних послуг, інтеграція розумного міста в систему взаємодії лікаря та пацієнта; громадська безпека – рівень злочинності, ступінь відповідальності правоохоронних органів, вплив новітніх технологій на це; продуктивність – міська політика та технології, спрямовані на підвищення продуктивності та можливості громадян всіх соціальних шарів отримувати доступ до цифрових послуг. За даними Juniper Research та Intel від 2017 року, саме Сінгапур провідним інтелектуальним містом у

світі та займає лідерство серед всіх вище описаних чотирьох напрямках. Найбільш розвинуті приклади міст представлені на рисунку 1.4:

The Top 20 Global City Performance by Index, 2017

	Mobility	Health	Safety	Productivity
1	Singapore	Singapore	Singapore	Singapore
2	San Francisco	Seoul	New York	London
3	London	London	Chicago	Chicago
4	New York	Tokyo	Seoul	San Francisco
5	Barcelona	Berlin	Dubai	Berlin
6	Berlin	New York	Tokyo	New York
7	Chicago	San Francisco	London	Barcelona
8	Portland	Melbourne	San Francisco	Melbourne
9	Tokyo	Barcelona	Rio de Janeiro	Seoul
10	Melbourne	Chicago	Nice	Dubai
11	San Diego	Portland	San Diego	San Diego
12	Seoul	Dubai	Melbourne	Nice
13	Nice	Nice	Bhubaneswar	Portland
14	Dubai	San Diego	Barcelona	Tokyo
15	Mexico City	Wuxi	Berlin	Wuxi
16	Wuxi	Mexico City	Portland	Mexico City
17	Rio de Janeiro	Yinchuan	Mexico City	Rio de Janeiro
18	Yinchuan	Hangzhou	Wuxi	Yinchuan
19	Hangzhou	Rio de Janeiro	Yinchuan	Hangzhou
20	Bhubaneswar	Bhubaneswar	Hangzhou	Bhubaneswar

The Top 20 Smart Cities Globally, Consolidated Performance 2017

	City	Region
1	Singapore	Asia Pacific
2	London	West Europe
3	New York	North America
4	San Francisco	North America
5	Chicago	North America
6	Seoul	Asia Pacific
7	Berlin	West Europe
8	Tokyo	Far East & China
9	Barcelona	West Europe
10	Melbourne	Asia Pacific
11	Dubai	Middle East & Africa
12	Portland	North America
13	Nice	West Europe
14	San Diego	North America
15	Rio de Janeiro	Latin America
16	Mexico City	Latin America
17	Wuxi	Far East & China
18	Yinchuan	Far East & China
19	Bhubaneswar	Indian Subcontinent
20	Hangzhou	Far East & China

Рисунок 1.4 – загальний та детальний рейтинги розумних міст за кожним з напрямків від 2017 року [3]

Перехід на протокол інтернету IPv6

Проблему вичерпання адресного простору для правильної маршрутизації пристроїв в мережах різних масштабів не слід забувати. Автоматизація буденних справ кожної людини потребує щонайменше 5-6 пристроїв, кожному з котрих необхідно надати власну IP-адресу. А якщо брати на увагу те, що кількість людей, які будуть використовувати пристрої з категорії «розумних» і не забувати про звичні мережеві пристрої, проблема стає очевидною.

Власне, сам протокол був створений ще у 1996 році, Google став активно його використовувати у 2005 році, а офіційний світовий запуск стався у 2015 році. Після запуску, аналітики завіряли, що через 5 років людство повністю позбавиться від пережитків минулого в обличчі IPv4 і повністю перейде на новий стандарт – IPv6. Проте, на сьогоднішній день, за даними Google, лише приблизно 35% всього трафіку приходиться на IPv6, що показано на рисунку 1.5:

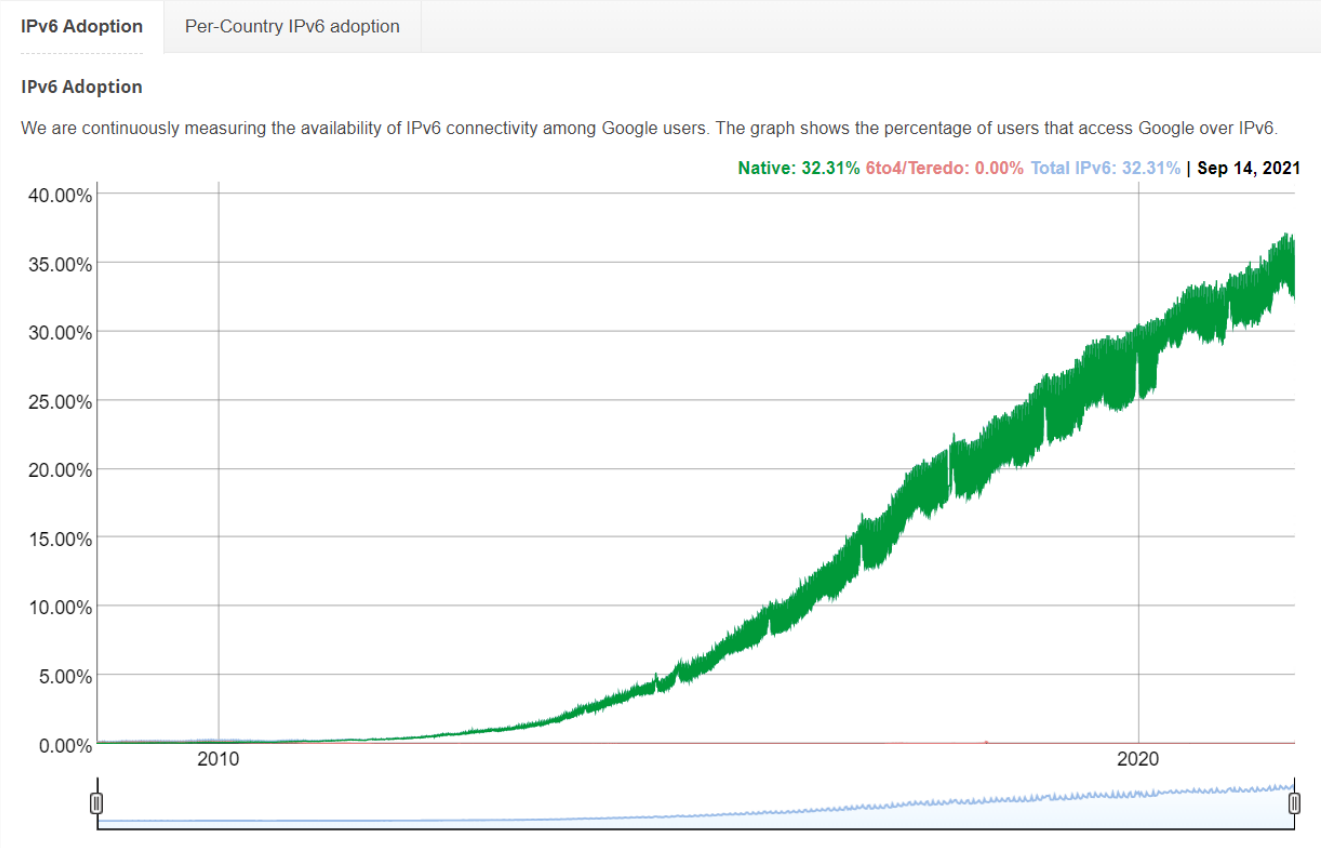

Рисунок 1.5 – Статистика використання IPv6 у світі [7]

Ситуація на вітчизняному ринку і того гірша. На відміну від країн, які намагаються розповсюдити новий стандарт, або такими, як Єгипет, де дуже гарно триває розгортання IPv6, проте користувачі не можуть повноцінно перейти на новий стандарт через проблеми з безпекою та швидкістю з’єднання, в Україні ситуація більш плачевна ситуація, аналітика стосовно якої представлена на рисунку 1.6:

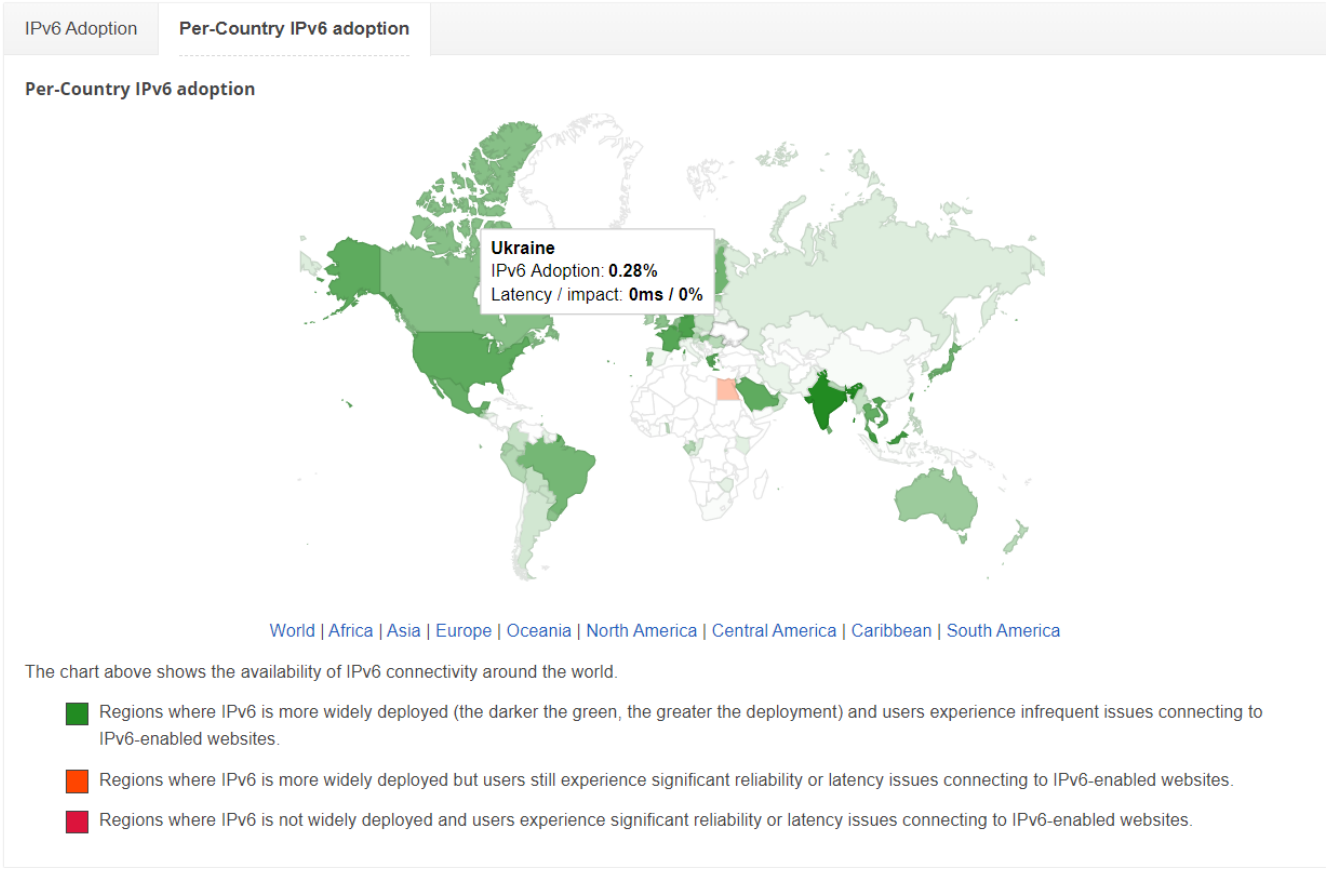

Рисунок 1.6 – рівень розповсюдження IPv6 в Україні [7]

Кількість підключених до мережі девайсів росте в геометричній прогресії і зараз вимірюється десятками мільярдів. За даними IDC, до 2025 року в мережі буде більш ніж 152 мільярди пристроїв тільки інтернету речей. На даний момент їх лише 10 мільярдів. Очікується приріст в 15 разів за 4 роки, що зображено на рисунку 1.7:

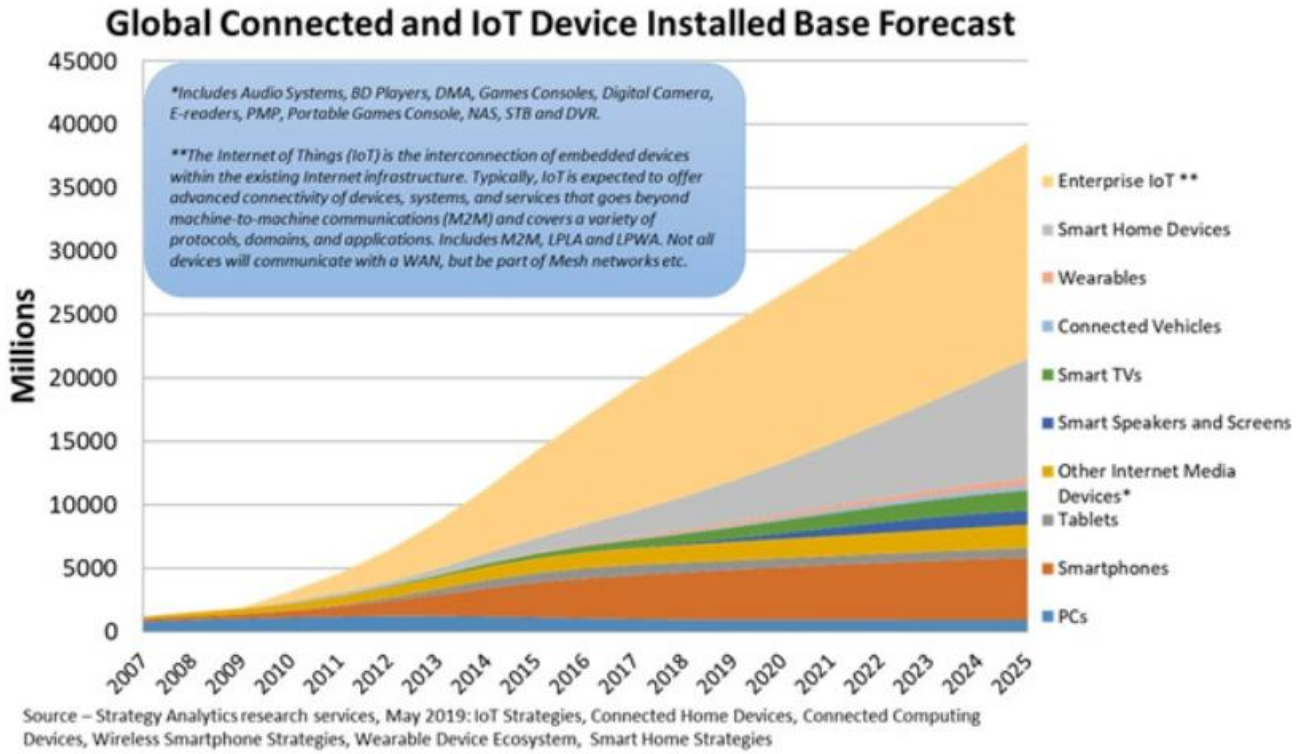

Рисунок 1.7 – Прогноз росту кількості підключених до мережі пристроїв у світі [8]

Майбутнє впровадження розумних технологій в проектування комп'ютерних мереж передбачає створення високої щільності пристроїв, які потребують власну IP-адресу. IPv6 позбавить від необхідності у використанні NAT (Network Adress Translation), кожен пристрій, який підключений до мережі, буде мати власну «білу» адресу і даний варіант вирішує проблему вичерпання IP-адрес на десятиліття вперед.

Не дивлячись на це, IPv6 має і ряд недоліків, через які досі не було повсюдного впровадження. Існують дві глобальні проблеми: відсутність зворотної сумісності з IPv4 та потреба у великих фінансових затратах. Далеко не всі пристрої пристосовані до нормальної роботи з використанням IPv6, а деякі взагалі не мають його підтримки. Невеликі компанії та провайдери малих мереж просто не мають відповідних фінансів і не можуть активно сприяти глобальному переходу.

Проте глобальний перехід на новий стандарт є безповоротним. Великі корпорації вже досить давно повністю перешли на IPv6, а серед країн, які активно впроваджують новий стандарт та сприяють прогресу лідирують США, країни Центральної Європи та Азії. Навіть не дивлячись на це, питання досі залишається невирішеним і над ним активно ведуться дискусії щодо правильного та поетапного впровадження, адже в умовах стрімкого збільшення кількості пристроїв IoT, найближчим часом навіть існуючих технологій не вистачить, щоб задовільнити майбутній трафік.

Стандарт 5G в рамках бездротових мереж

Використання нового покоління зв'язку 5G стане рішучим етапом у подальшому розвитку концепції «розумного міста». 5G – це більше, ніж просто пропускна здатність чи швидкість з'єднання. Новий стандарт зв'язку буде використовувати мобільні технології з точки зору параметрів передачі даних, аналогічних широкосмуговому з'єднанню. Важливою перевагою, в порівнянні з існуючою технологією, стане можливість обробляти велику кількість пристроїв та датчиків на невеликій площині без затримки. Нове покоління зв'язку має низку переваг та актуальних нововведень, але оглянемо лише ті, які стосуються інтернету речей, розумних будинків та міст. Інфографіка розвитку та популяризації 5G представлена на рисунку 1.8:

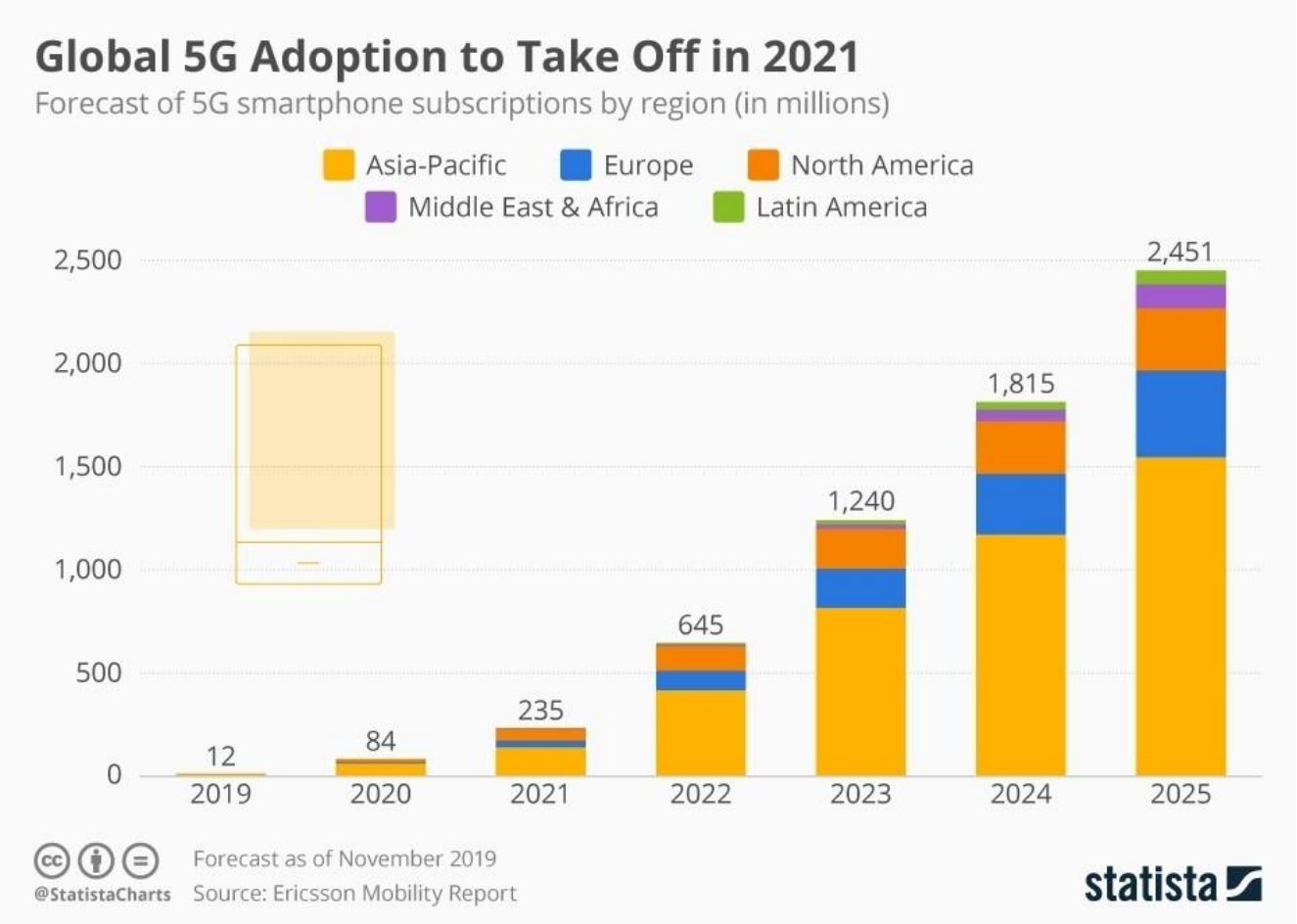

Рисунок 1.8 – Розвиток та популяризація 5G у світі [9]

У контексті четвертої промислової революції, основною силою якої стане обробка та обмін даними, обслуговування до 100 пристроїв та датчиків на одному квадратному метрі є особливо важливим. Датчики, які збирають інформацію про навколишнє середовище, будуть встановлені на автомобілях, дорогах, годинниках, одягу та багатьох інших пристроях, які будуть використовувати технологію 5G для зв’язку. Саме зв’язок датчиків інтернету речей є важливим елементом у подальшому розвитку технологій розумного будинку. Порівняння стандартів зв’язку 4G та 5G представлено на рисунку 1.9:

4G		5G
100 Мб/с – 1 Гб/с	**Швидкість сигналу**	1 Гб/с – 11 Гб/с
3–19 км	**Діапазон покриття без значної втрати швидкості**	до 1 км
60–98 мс	**Затримка**	до 1 мс
2000 на кв.км.	**Середня кількість одночасних підключень**	1 млн на кв.км.
до 6 ГГц	**Частоти**	30 – 300 ГГц

Рисунок 1.9 – переваги та недоліки в порівнянні двох стандартів [10]

Серед очевидних переваг : космічна різниця у швидкостях, враховуючи, що 4G досить непогано задовільняла потреби, дуже низька затримка та космічна кількість можливих активних підключень. Проте слабким місцем 5G є те, що всі ці неймовірні показники можливі лише при відсутності будь-яких перешкод та знаходженню у дозволеному діапазоні від точки сигналу. Розповсюдження нового покоління потребує встановлення великої кількості точок доступу у вигляди радіочастотних вишок або антен. Проте, як і з переходом з IPv4 на IPv6, це також можна назвати, свого роду, безповоротною подією, яка колись все-одно трапиться.

1.3 Існуючі методи керування комп’ютерною мережею

Керування комп’ютерною мережею – виконання багатьох функцій, необхідних для контрою, планування, виділення, впровадження, координації і моніторингу ресурсів комп’ютерної мережі [11]. Вони включать в себе начальне мережеве планування, розподілення частот, передвизначення маршрутів трафіку для підтримки балансування навантаження, керування конфігурацією, відмовостійкістю, безпекою, продуктивністю та обліком інформації.

Основна причина постійного нагляду за тим, що відбувається у мережі і якомога швидше означати всілякі проблеми, є те, що працездатна комп’ютерна мережа стала невід’ємно важливою для функціонування підприємств. Ціною за

простій у роботі мережі можуть бути втрачені впусту робочі часи, зруйновані ділові зв’язки та репутація.

Одним з перших способів управління мережевими ресурсами було використання віддаленого доступу до комп’ютера або іншого мережевого вузла з метою його адміністрування, але з плином часу збільшилися масштаби мережі, кількість мережевих пристроїв та клієнтських вузлів, а також більш складні інструменти керування мережею.

Міжнародна організація по стандартизації описала FCAPS модель, в якій відображені ключові функції адміністрування та керування комп’ютерною мережею [11]:

- (F) Fault Management / керування відмовами
- (C) Configuration Management / керування конфігурацією
- (A) Accounting Management / облік роботи мережі
- (P) Performance Management / керування продуктивністю
- (S) Security Management / керування безпекою

Задачі керування відмовами – виявлення, визначення та усунення наслідків збоїв та відмов в роботі мережі.

Керування конфігурацією полягає в безпосередньому конфігуруванні компонентів мережі, включаючи їх місцерозташування, мережеві адреси та ідентифікатори, керування параметрами мережевих операційних систем, підтримка схеми мережі.

Облік роботи мережі включає в себе реєстрацію та керування ресурсами та пристроями. Також необхідною складовою є ведення мережевого журналу, в якому описується початковий стан мережі та всі наступні зміни у ній в хронологічному порядку.

Керування продуктивністю слугує для представлення статистики роботи мережі в реальному часі, мінімізації заторів та вузьких місць, виявлення

виникаючих тенденцій та планування ресурсів для майбутніх потреб. Керування продуктивністю комп'ютерної мережі охоплює наступні аспекти[12]:

- Збір статистики використання пристроїв
- Визначення порогу сповіщення (Notification Threshold)
- Процедури тестування та симуляції
- Виконання звітності

Керування безпекою включає в себе контроль доступу та збереження цілісності даних. В функції також входить процедура автентифікації, перевірки привілеїв, підтримка ключів шифрування, керування повноваженнями. До цієї ж групи можна віднести важливі механізми керування паролями, зовнішнім доступом, з'єднання з іншими мережами. В керуванні інформаційною безпекою застосовують засоби та системи керування мережею, які дозволяють встановити, попередити та протистояти можливим атакам та іншим загрозам безпеки. Забезпечення безпеки мережі починається з визначення критично важливої інформації, можливо пріоритетність захисту для кожного з варіантів передачі та типу інформації. Після цього необхідно ідентифікувати всі канали доступу: термінальні послуги, FTP/HTTP сервери, розподілення мережі і все, що пов'язано з наданням доступу до неї, включаючи DNS. Основні варіанти застосування безпеки мережі відрізняються рівнем втілення: на рівні каналу передачі даних можна використовувати криптографію, шифруючи важливі дані; на рівні мережі, дозволяючи лише пріоритетний трафік, фільтруючи пакети; на рівні застосунків, за допомогою безпечної та стійкої процедури автентифікації.

Сучасні методи керування мережею повинні виконувати та задовольняти наступні потреби [13]:

- Відстеження збоїв у всіх мережевих пристроях, визначення та усунення їх причин, виправлення їх наслідків та попередження збоїв в майбутньому (наприклад, виконанням діагностичних операцій)

- Управління конфігуруванням комп’ютерів та мережевих пристроїв (ініціалізація, переконфігурування і т.д.)
- Керування споживанням мережевих ресурсів користувачами та групами користувачів (встановлення меж дискового та хмарного простору на кожного окремого користувача та, наприклад, загальногрупову папку)
- Керування продуктивністю мережевих пристроїв та сервісів
- Керування захистом даних за допомогою контрою доступу до мережевих ресурсів на основі заздалегідь встановленої політики безпеки

В загальному вигляді, побудована мережа керується за допомогою застосунку по її керуванню, який має доступ до адміністрування як мережевих пристроїв, так і окремих вузлів самої мережі. Даний типовий застосунок може виконуватися на робочому місці мережевого адміністратора або на іншому комп’ютері (наприклад, домашньому комп’ютері адміністратора для вирішення певних проблем після робочого дня, або на комп’ютері одного з клієнтів). Його назначення може варуватись від потреб компанії або положень політки безпеки, але основною метою є збір даних про керовані пристрої, які поступають від так званих агентів – додатків або сервісів операційної системи. Зазвичай, програма для керування мережею оперує великими об’ємами даних і за допомогою користувальницького інтерфейсу консолі керування, доступної мережевому адміністратору, оброблює мережеві події, які виконуються в даний момент [13]. Також в основний функціонал входить запуск тестів, на основі зібраних даних, конфігурація чи переконфігурація, діагностика. Для взаємодії таких додатків з агентами, зазвичай, використовуються відкриті мережеві протоколи, такі як SMNP (Simple Network Management Protocol) в локальних мережах та CMIP (Common Management Information Protocol) у розподілених мережах, які використовують телекомунікації. Проте, за необхідністю, певні виробники програмного забезпечення користуються власними мережевими протоколами.

1.4 Висновки за розділом

В даному розділі буди розглянуті існуючі рішення, теорії та концепції стосовно керування комп’ютерними мережами та їх положенням у цілому. Описані методи носять загальний характер та підлягають опрацюванню та створенню єдиного рішення в рамках проекту.

Даний розділ є оглядовим та носить дослідницький характер, що полягає у визначенні існуючих моделей та дослідження їх основних постулатів з метою формування власної думки та концепції, стосовно ознайомленого матеріалу.

Наступний розділ буде присвячений теоретичному опису ідеї проекту та порівнянні з існуючими, з відкритим доступом, аналогами.

2. ТЕОРЕТИЧНЕ ОБҐРУТНУВАННЯ

2.1 Обґрунтування напрямку дослідження

Дослідження проводиться з метою виявлення недоліків у методах управління комп'ютерною мережею. Напрямок був обраний виходячи з аналізу сучасних методів управління, їх недоліків та зауважень до них. Робота націлена вирішити проблеми управління комп'ютерною мережею, спонукає до визначення методів управління на етапі моделювання, більш доцільно використовувати людський ресурс на кінцевому етапі та підтримці працездатності мережі та запропонувати об'єднаний комплекс рішень по доцільному управлінню готовою мережею, який буде задовольняти потреби як розподілених мереж корпоративного масштабу, так і невеликих локальних мереж.

2.2 Методика проведення наукового дослідження

За основу дослідження взята запропонована ідея по управлінню проектом концепції «розумного» міста. Наукове дослідження було побудоване на аналізі існуючих рішень у галузі мережевих технологій та телекомунікацій, їх порівнянні між собою, об'єднанні найкращих аспектів з них та висунення запропонованого рішення, як найбільш доцільного.

Після виявлення основних проблем та постанови потребуючих вирішення питань, були обрані методи їх вирішення та постанова ходу дослідження, поділеного на етапи та описаного в таблиці 2.1.

Таблиця 2.1 – Етапи наукового дослідження.

Етап дослідження	Результати
1. Вибір та опис напрямку дослідження.	Була створена мета дослідження, обраний об’єкт дослідження.
2. Дослідження джерел інформації стосовно ідеї.	Аналіз інформації у галузі мережевих технологій та телекомунікацій, та структурування отриманих результатів.
3. Дослідження концепції «розумного» міста.	Був проведений аналіз концепції на предмет методів керування та основних ідей взагалі. Виявлені проблеми та переваги.
4. Аналіз існуючих рішень стосовно напрямку дослідження.	Огляд рішень від різних компаній, їх порівняння між собою, виявлення переваг та недоліків. Були обрані найкращі практики.
5. Дослідження суміжних технологій на предмет втілення їх у проект.	Аналіз технологій стандарту зв’язку 5G та протоколу IPv6. Визначення переваг та проблем у втіленні їх у проект. Опис майбутнього втілення у проекти по створенню комп’ютерних мереж.
6. Створення єдиного теоретичного рішення по управлінню комп’ютерними мережами.	Покроковий опис по впровадженню доцільного рішення по управлінню комп’ютерними мережами на прикладі проекту «Розумне місто»
7. Моделювання	Була створена модель «розумного» міста з використанням запропонованого рішення по його управлінню.

2.3 Опис та хід наукового дослідження

Методи управління мережею

Проаналізувавши джерела інформації та оцінивши рішення по управлінню комп'ютерними мережами, була виявлена проблема в організації працездатності та відмовостійкості мережі, а також надлишковий або невірний підхід до створення методів управління.

Перш за все слід зрозуміти, що 100% відмовостійких систем не існує. Проблеми звичайного користувача або співробітника будь-якого характеру (недоступний інтернет, проблеми з авторизацією, гальмує RDP) вирішуються так званим реактивним методом. Його характеристика полягає в усуненні проблеми, яка вже сталась. Для обслуговування великої мережі, особливо розподіленої, реактивний підхід виявляється недостатнім. З плином часу проблеми починають накопичуватися наче сніжний ком. Оскільки, на сьогоднішній день, працездатна мережа є невід'ємною частиною як буденного життя, так і працездатності багатьох, якщо не всіх, фірм та корпорацій.

Для максимально можливого усунення неочікуваних відмов у мережі слід використовувати комплексний та структурний підходи по управлінню мережею. Загалом, задача по управлінню мережею може бути розподілена на дві складові:

- Структуровані роботи – заплановані заходи по підтримці мережі
- Реактивні роботи – дії по усуненню виявлених відмов

На жаль, в реальній мережевій інфраструктурі неможливо повністю усунути реактивні роботи по усуненню проблем, проте структурований підхід дозволяє якщо не звести їх до мінімуму, то кардинально зменшити. Судячи з аналізу існуючих рішень, де застосовується в більшій мірі реактивний підхід та тих, де переважають структуровані події та очікувана поведінка мережі, реактивні роботи

проводяться так чи інакше, десь в більшій мірі, десь в меншій, проте повністю усунення таких робіт не є можливим.

Для підтримки працездатності мережі та опис способів по її управлінню описаний в моделях великих корпорацій (Cisco Lifestyle Services, TMN, FCAPS, ITIL). Проте запропоновані методи, по загальним оцінкам людей, які втілили реалізацію у власні проекти, є лише опорним пунктом для створення структурованої моделі по управлінню, причиною чого є або недостатність критично важливих аспектів, або навпаки велика надлишковість процедур.

Основний спосіб управління мережею – командний рядок (CLI), проте сьогодні в основному користуються застосунками з графічним користувальницьким інтерфейсом (GUI). Варіативність у виборі програмного забезпечення масштабна, проте це викликано перевагами одного продукту над іншим в галузі кількості керованих пристроїв, можливостях, портативності і так далі. Задача по управлінню комп'ютерною мережею стоїть критичним питанням, особливо при великих територіально розподілених мережах. Способи управління можуть бути організовані по тим самим каналам, по яким передається користувальницький трафік, через окремий керований порт або по виділеним каналам з хмари. Важливо зауважити, що доступ до мережевих пристроїв критично важливий не тільки для управління, але й для системи моніторингу стану мережі.

Моніторинг мережевої інфраструктури можна поділити на наступні складові:

1. Моніторинг мережевих пристроїв
   1.1 Збір системних повідомлень
   1.2 Моніторинг доступності та телеметрії мережевого пристрою
   1.3 Сповіщення про змінах у мережі
2. Моніторинг каналів передачі даних

Моніторинг мережевої інфраструктури дозволяє володіти всією необхідною інформацією, стосовно мережі в режимі реального часу, а також визначати робочий рівень (baseline) для параметрів різних мережевих пристроїв. Для різних структур

мережі, вузлів, в яких знаходиться пристрій та його важливості даний рівень може бути різним. Наприклад, в одному вузлові знаходиться маршрутизатор, на який надходить інтернет і його задача просто передати цей сигнал на декілька комутаторів. Для такого маршрутизатора навантаження на процесор в межах 10% в нормальному режимі роботи – задовільний стан, а щодо комутаторів, які можуть бути і на 48 + 8 керованих портів, навантаження на процесор може бути в межах 30-40% і це буде вважатися задовільним станом, при якому система працює. Саме для визначення такого стану допомагає моніторинг: виявивши робочий рівень мережевого пристрою, можна легко розпізнати можливі проблеми в системі, коли він змінюється і не лише в більшу сторону. Якщо зауважені не всі запропоновані пункти, то може виявитися, що на момент виникнення чергової проблеми, виявиться критична нехватка інформації, що потребує додаткового часу на введення системи в робочий стан. Моніторинг стану, в межах описаних вище задач, є необхідною і достатньою умовою працездатності комп'ютерної мережі на належному рівні. Володіння отриманою інформацією дозволяє впоратися майже з будь-якою проблемою у стислі строки, а більшість проблем може бути вирішено проактивно, тобто ще до виникнення відмови.

З плином часу надійність мережевих пристроїв знижується: застарілі обладнання схильні до нових атак, мережа стає вразливою. Крім того, застарілі пристрої перестають задовольняти стрімко зростаючим потребам у продуктивності та функціональності. Необхідно мати вичерпуючу інформацію про поточний стан мережевих пристроїв, критично оцінювати ймовірність та час повного старіння та, за необхідності, здійснювати заміну на більш сучасний пристрій. Також важливо мати запасні пристрої на випадок неочікуваного виходу з ладу одного з них, щоб провести заміну хоча б на деякий час. Також, важливо додати, що виробники програмного забезпечення постійно розробляють нові версії операційних систем для мережевого обладнання. Зазвичай в них вирішуються вразливості, додаються нові функції, підвищується продуктивність. Оновлення програмного забезпечення з застарілого на новітнє є не менш важливим, ніж сама заміна пристрою.

Необхідним аспектом у структурованому підході по управлінню комп’ютерною мережею є резервне копіювання. При відмові пристрою, зазвичай втрачається опис його конфігурації. Заміна обладнання на більш нове, описана вище, потребує встановлення конфігурації старого пристрою для нормальної роботи системи. Налаштовувати пристрій спочатку, згадуючи на ходу всі нюанси, коштує часи простою системи, але задача значно спрощується за наявності резервної копії конфігурації минулого пристрою. Корисність даного аспекту не обмежується лише цим. Оновлення конфігурації або зміна певних налаштувань на мережевому пристрої може привести до збою, причиною чого може бути не тільки людський фактор, але й виникнення неочікуваної помилки у програмному забезпеченні. За наявності резервної копії конфігурації до початку внесення у неї змін, відновити працездатність мережі чи її функціонал може бути виконана у стислі строки. Після відкату до минулої стабільної версії можна визначити помилку в новій конфігурації.

Зміни в мережі так чи інакше відбуваються. З моменту її створення виникає і перша документація, куди необхідно вносити всі подальші зміни в налаштуванні і топології мережі та її модернізації в процесі експлуатації. Відсутність документації ускладнює підтримку , пошук та усунення несправності мережі, якою займаються, як правило, декілька людей, кожен з яких вносить свої зміни.

Після огляду основних операцій в ході управління комп’ютерною мережею маємо перелік критичних рішень, впровадження котрих має ключове значення у подальшій роботі мережі та її відмовостійкості. Проаналізувавши існуючі рішення був отриманий алгоритм дій з моменту впровадження самої мережі до її обслуговування, зображений на рисунку 2.2:

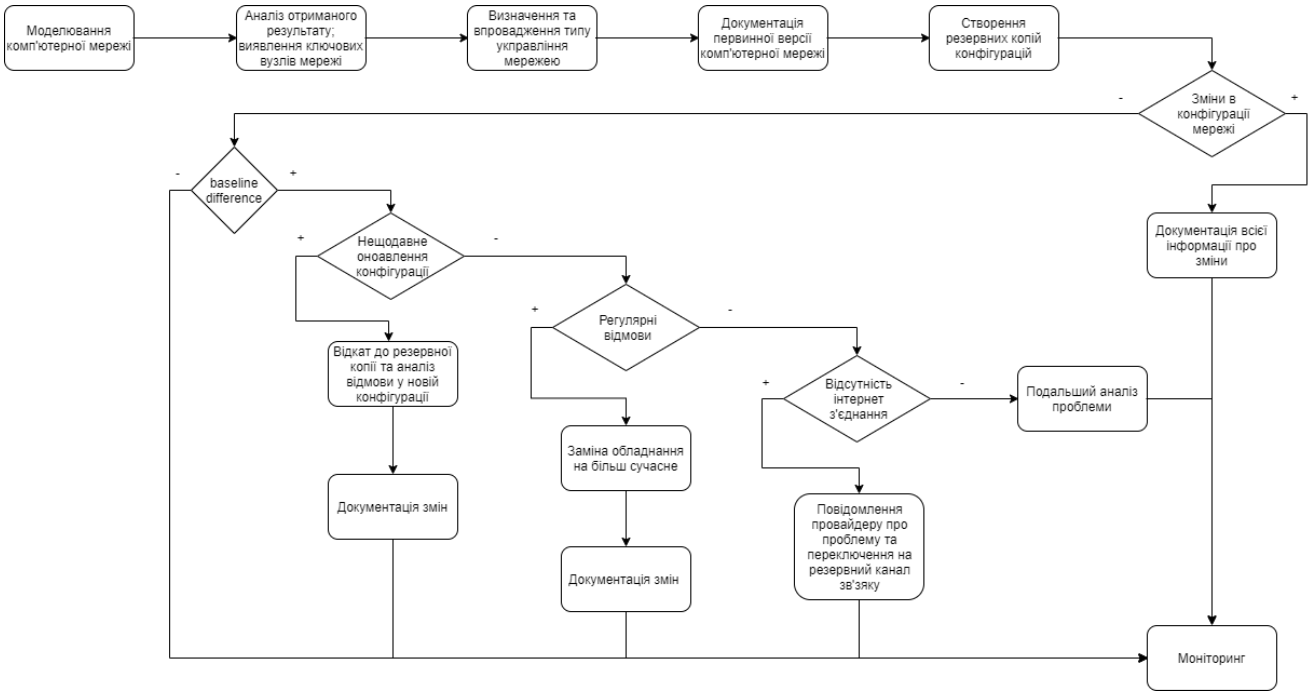

Рисунок 2.2 – алгоритм управління комп’ютерною мережею

Моделювання комп’ютерної мережі втілює собою відправну точку, адже осмислення необхідності керування мережею виникає не одночасно з ідеєю її втілення. Далі слід проаналізувати змодельовану мережу та визначити її ключові вузли, наділяючи їх особливою увагою. Наступним кроком є визначення та впровадження методу управління. Проаналізувавши існуючі рішення та скомбінувавши для різних вузлів або ділянок мережі, впровадити їх. Слід задокументувати отриманий первинний варіант мережі, щоб в подальшому відстежувати можливі проблеми при зміні топології мережі, маючи перед собою її первинний та наступні працездатні варіанти. Фінальним кроком виступає моніторинг мережі в режимі реального часу. На практиці – це основна операція в структурованому управлінні мережею. Саме моніторинг дає вичерпну інформацію про поточний стан мережі та допомагає запобігти великої кількості відмов. Надалі описаний важливий крок по документації будь-яких змін в мережі: чи то зміни в топології, чи в конфігурації одного або декількох мережевих пристроїв, або їх заміна на нові.

Далі описані найбільш часті проблеми, з якими доводиться стикатися при управлінні комп'ютерною мережею. У випадку відмови спочатку необхідно проаналізувати поточний стан, перш ніж приступати до дій. Відправною точкою слугує показник baseline (робочий рівень). Після первинного налаштування мережі шляхом її моніторингу на початку роботи визначається робочий рівень для кожного пристрою, тобто так зване навантаження на пристрій, при якому він працездатний. Під час моніторингу його легко відстежити по навантаженню на центральний процесор пристрою: якщо він в рамках визначеної норми, то слід продовжити моніторинг, але якщо він відрізняється, в більшу (перенавантаження або надлишкова кількість пакетів чи паразитного трафіку) чи меншу (можливо при апаратній відмові, виходу з ладу одного чи більше портів або банальній відсутності інтернет з'єднання) сторону, то необхідно шукати причину.

Одним з варіантів може бути проблема в нещодавньому оновленні конфігурації пристрою. В даному випадку слід повернутися до минулої конфігурації або в крайньому випадку замінити пристрій на аналогічний. Після цього, коли мережа знову працездатна, слід задокументувати проблему та можливі зміни в мережі і можна присвятити час аналізу відмови у новій конфігурації та продовжити моніторинг.

Постійні відмови пристрою також доволі часта практика. У випадку якщо пристрій часто виходить з ладу по будь-яким причинам (зазвичай це незначні відмови, які усуваються без втручання за декілька хвилин) необхідно провести заміну пристрою та задокументувати задіяні зміни. Часті відмови характерні для застарілого обладнання, тому втрачати час на пошук несправності не є релевантним і слід продовжити моніторинг.

Найбільш банальною, проте не менш частою, проблемою є відсутність інтернет з'єднання. Оперативне усунення даної проблеми можливе лише за наявності резервного каналу зв'язку від іншого провайдера. Це вважається нормальною практикою, проте не має повсюдного втілення (наприклад на датчиках чи пристроях безкоштовного громадського інтернету). В даному випадку слід

проаналізувати пристрій, на який приходить інтернет, можливо в ньому не працює саме той порт, на який поданий канал зв’язку. Проте це скоріше виняток і слід просто проінформувати постачальника інтернет-послуг про несправність.

Перераховування всіх можливих проблем не втілити в алгоритм, адже, не дивлячись на прагнення до створення універсального способу управління комп’ютерною мережею, не всі відмови мають однаковий характер та спосіб їх усунення. Тому подальший аналіз повинен будуватися на особистій практиці відповідальної за стан мережі людини та створеній документації.

Порівняння методів управління комп’ютерною мережею

Для уникнення подальших проблем з вибором методу подальшого управління комп’ютерною мережею, слід ще на етапі моделювання визначитися з напрямком її побудови та передбачити можливі зміни та модернізації, щоб прийти до кінцевого рішення. Можна виділити декілька методів управління мережевим обладнанням. До класичних методів відносяться управління по основній мережі, використовуючи ті самі канали, по яким йде користувальницький трафік (in-band) та по зовнішньому каналу (out-of-band) [14]. Також існують й альтернативні варіанти управління, наприклад, за допомогою хмарних технологій. Його принцип має спільні характеристики з описаними вище технологіями, проте через його гібридність, він знаходиться особняком. Також величезну популярність та попит набирає концепція програмно-визначених мереж (SDN). Для подальшого вибору слід визначити переваги кожного методу.

Перший метод управління мережею (in-band), основна ідея якого зображена на рисунку 2.3, передбачає передачу трафіка по управлінню мережевим обладнанням (SSH, HTTPS, Telnet та інші) та засобами моніторингу мережі (Syslog, SNMP, Netflow та інші) через ті самі канали, якими передається весь користувальницький трафік.

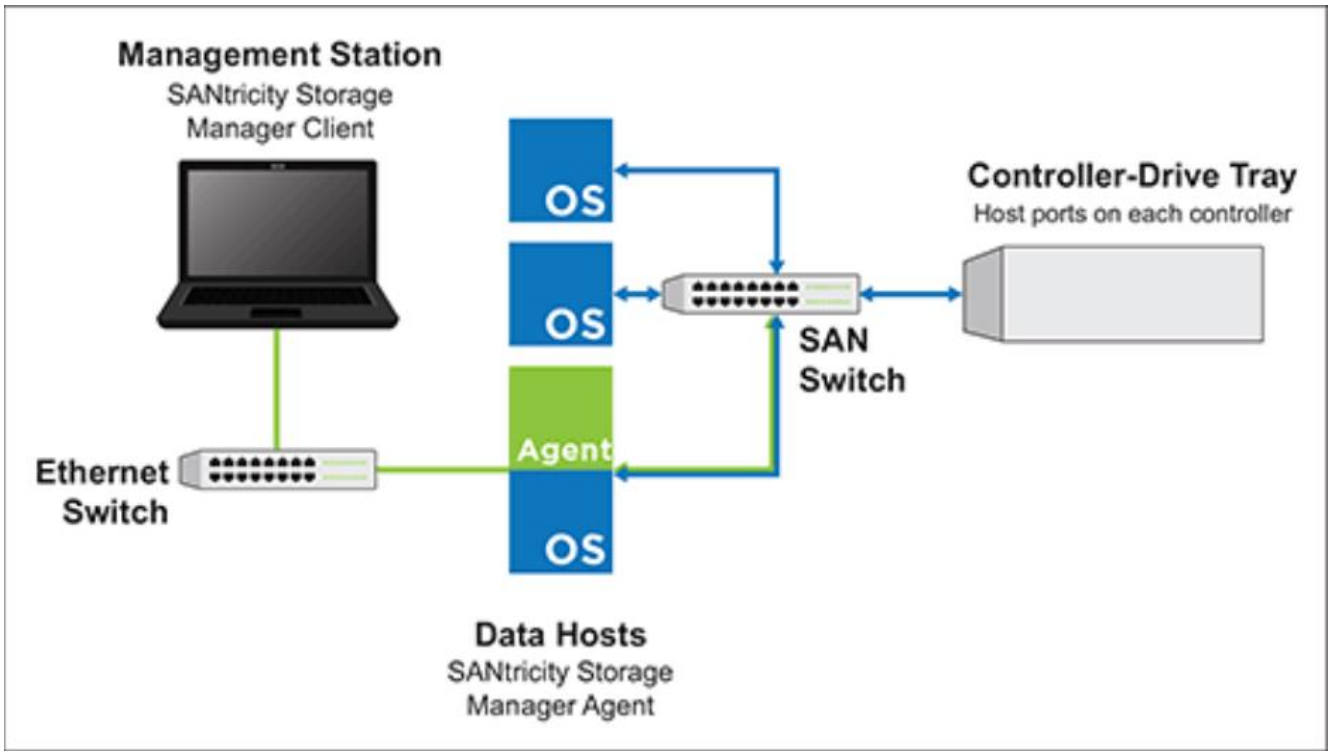

Рисунок 2.3 – метод управління комп’ютерною мережею in-band [15]

Для такого варіанту необхідно на логічному рівні сегментувати трафік управління та користувальницький, адже все відбувається в рамках однієї мережі. Способи реалізації можуть бути різними: списки доступу (Access-List’s), віртуальні мережі (VLAN), користування міжмережевими екранами тощо. Проте, на справі, фізична інфраструктура залишається такою самою. Перевагою даного рішення є простота. Проте простота полягає лише у первинному налаштуванні. Тривала робота з даним методом управління мережею загрожує проблемами з усуненням відмов у мережі. Наприклад, у випадку відмови певного сегменту мережі (наприклад, збій через велику кількість паразитного трафіку), доступ до мережевих пристроїв може бути перекритим, що ускладнює діагностику та виявлення проблеми. Щоб уникнути такої проблеми необхідно налаштовувати різні рівні якості обслуговування трафіку (QoS). Трафіку моніторингу та управління надати високий пріоритет, виділив мінімальну пропускну здатність. Промаркований таким чином трафік буде передаватися мережею, навіть якщо вона перенавантажена. Проте, навіть такі операції не дають 100 відсоткової гарантії, що пристрій по

невідомій причині не заблокує перенавантажений порт і не зникне віддалений доступ до нього.

Другий метод управління (out-of-band) передбачає передачу трафіку управління через окремі фізичні канали зв'язку, для чого будується друга мережа і на кожному ключовому пристрої відводиться окремий порт для підключення до неї. Також встановлюється додатковий комутатор для підключення до нього всієї інфраструктури управління мережею [16]. В даному варіанті доступ до управління мережею буде забезпечений наскільки це можливо: доступ до управління мережевими пристроями буде забезпечений навіть у випадку виходу з ладу основної мережі. Принцип роботи зображений на рисунку 2.4:

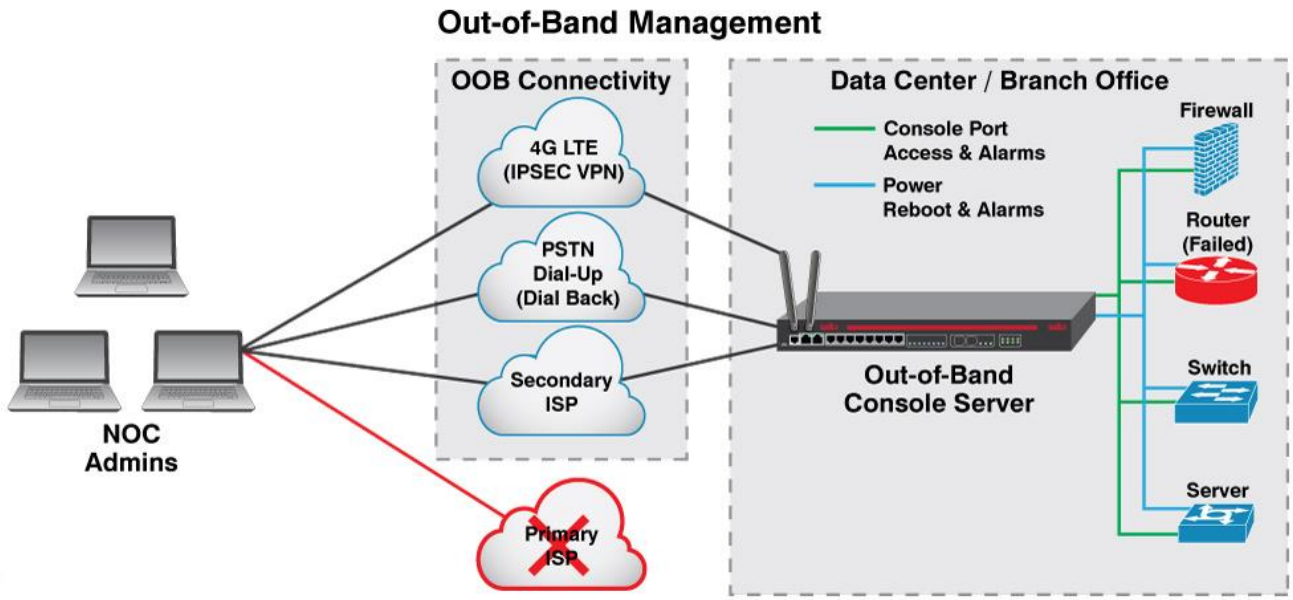

Рисунок 2.4 - метод управління комп'ютерною мережею out-of-band [17]

Даний метод є практичним усуненням недоліку минулого in-band, проте і сам не позбавлений недоліків. Основним недоліком прийнято вважати необхідність у використанні додаткового обладнання для створення другої мережі та виконання додаткових налаштувань на всіх пристроях для реалізації методу. Крім того існує постійна необхідність в окремих каналах зв'язку. При розташуванні всього мережевого обладнання в рамках одного серверного приміщення такої проблеми

не буває, але, у випадку територіально-розподілених мереж, проблема отримання додаткових каналів стає критичною. Окрім проблеми у прокладці додаткових мідних чи оптичних трас, не кожний пристрій оснащений додатковими портами для підключення до мережі управління.

Таблиця 2.5 – порівняння методів управління in-band та out-of-band [18].

In-band	Out-of-band
Доступ за допомогою Telnet/SSH	Доступ за допомогою консольного підключення
Залежить від IP-адреси та номера порту Telnet/SSH	Залежить від IP-адреси та номера порту, який був налаштований для доступу
Працює, коли мережеве з'єднання встановлено	Альтернативний доступ, коли мережа не працює
Синхронний	Асинхронний
Швидкість з'єднання висока	Швидкість з'єднання мінімально необхідна
З'єднання встановлюється через застосунки типу putty, Secure CRT	З'єднання встановлюється через термінальний доступ
Не потребує фізичного доступу	Не потребує фізичного доступу, оскільки доступна комутуєма лінія зв'язку

Маючи власні переваги та недоліки, жоден з вище описаних методів управління на практиці не є самодостатнім єдиним рішенням. У випадку територіально розподіленої мережі з простою топологією, використовувати out-of-band не є вигідним рішенням. Саме тому класична практика полягає у гібридному використанні цих методів. Також слід відмітити практику використання

консольного серверу, до якого підключаються всі мережеві пристрої. Перевага даного рішення полягає в тому, що навіть у випадку, коли пристрій не зміг нормально завантажитися, доступ до нього буде забезпечений. Проте розглядати його як єдине рішення заважать пара нюансів. До консольного серверу зручно підключати пристрої, які знаходяться в безпосередній близькості до нього, тобто в одній серверній кімнаті. Також консольне підключення непридатне до моніторингу мережевого обладнання і має низьку пропускну здатність, що впливає на швидкість передачі даних.

Використання хмарного управління мережею являє собою, в певному сенсі, гібридний метод управління. Одним із прикладів реалізації даного методу управління є лінійка продукції Cisco Meraki, концепція якої зображена на рисунку 2.6:

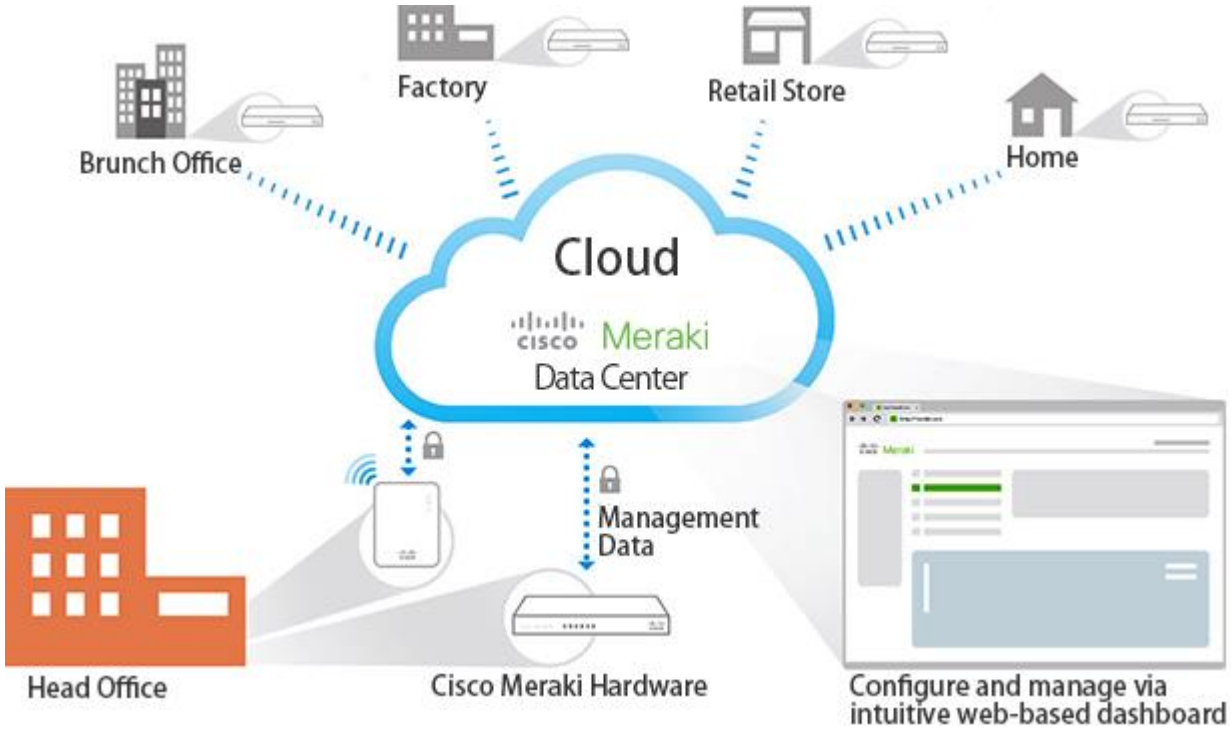

Рисунок 2.6 – концепція роботи з використанням мережевого обладнання Cisco Meraki [19]

Всі пристрої даної лінійки після підключення автоматично підключаються до хмари Cisco. Управління ними здійснюється через хмарний портал. Дана технологія користується популярністю, конкуруючи з SDN. Недоліком даного методу є втрата можливості управління у випадку втрати зв'язку. Саме тому з використанням даного методу суттєво підвищуються вимоги до надійності та кількості інтернет каналів. Також слід зауважити, що управління таким чином можливо лише за наявності в мережі необхідних пристроїв, а також те, що управління не розповсюджується на інші моделі обладнання.

Концепція програмно-визначених мереж (SDN) стрімко набирає оберти. Вона передбачає повне розділення функцій управління обладнанням та контролю трафіку від передачі даних. Таким чином, за управління всіма мережевими пристроями та логіку контролю за трафіком (протоколи маршрутизації, службові протоколи, VLAN) буде відповідати певний централізований програмний пристрій, а мережеве обладнання буде займатися тільки передачею даних. Перевага даного методу очевидна – управління всією мережею та дуже гнучка функціональність. Проте недоліком є факт того, шо не кожний мережевий пристрій обладнаний підтримкою даної технології.

Проте, з плином часу дана концепція набере оберти та стане кращим вибором у втіленні корпоративних WAN мереж. Існуючі рішення вже показують позитивний досвід впровадження та переваги. Рішення компанії InfoVista Ipanema слугує для формування трафіку та його пріоритету на прикладному рівні, щоб якомога ефективно оптимізувати продуктивність критично важливих додатків [20]. Cisco SD-WAN пропонує наглядні переваги втілення свого рішення у вигляді статистичних порівнянь [21]:

- Зниження вартості підключення на 65%
- На 33% більш ефективне управління WAN
- На 59% швидше впровадження нових сервісів
- На 58% швидше впровадження змін політики та конфігурації
- На 94% зменшення незапланованих простоїв

- На 48% зниження затримки додатків

Повсюдне втілення концепції SD-WAN, як і 5G та IPv6, лише питання часу, оскільки має очевидні переваги. Також вагомим аргументом є підвищення запитів по продуктивності мережі, процесу її масштабування та визначення способів управління нею.

Обґрунтування використання гібридного методу управління

Розподілення певних вузлів мережі на різні методи управління має сенс у випадку надання ним необхідної продуктивності: максимально можлива, мінімально необхідна або просто достатня. У випадку використання запропонованої мережі, для реалізації виконання описаних вище операцій, так чи інакше, потребується наявність певної кількості пропускної здатності. Моніторинг всіх мережевих пристроїв, відстеження їх робочого рівня, представляють собою спілкування між пристроєм, яке передає дану інформацію, та пристроєм, яке її збирає. В масштабах домашньої мережі, кількістю затраченого ресурсу можна знехтувати, проте працюючи з корпоративною мережею міського масштабу, кожний пристрій якої повинен повідомляти про свій поточний стан, втрати можуть бути суттєвими, особливо, якщо кількість користувальницького трафіку настільки ж велика, як і масштаби мережі та потребує своєчасної передачі.

За ефективністю будемо визначати пропускну здатність каналів зв’язку при необхідності регулярного їх використання для користувальницьких потреб та для забезпечення максимально можливої працездатності мережі за рахунок виконання проактивних операцій управління.

В ідеальній мережі кількість інформації, яка передається через канали зв’язку, не залежить від факторів колізії, інтерференції, втрати пакетів тощо. В реальних мережах на описані вище фактори витрачається приблизно 5-6% ресурсу

від заявленого показника. Додаючи до цієї втрати наявність трафіку по управлінню, отримуємо небажану суттєву втрату ресурсу.

Для визначення впливу сигналів управління та моніторингу на пропускну здатність, проведемо порівняння варіантів з одночасним трафіком управління та без нього на одному з вузлів реальної мережі. За приклад мережі з управлінням через ті ж канали зв’язку, по яким йде користувальницький трафік, розглянемо вузол корпоративної мережі. Задовільна та доступна для таких масштабів швидкість з’єднання приблизно дорівнює 500 Мбіт/с. В серверному приміщенні знаходяться 4 керованих комутатори 3 рівня приблизно на 80 робочих місць, кожне з яких потребує гарного, а головне надійного з’єднання. Структурна схема даного вузла представлена на рисунку 2.7:

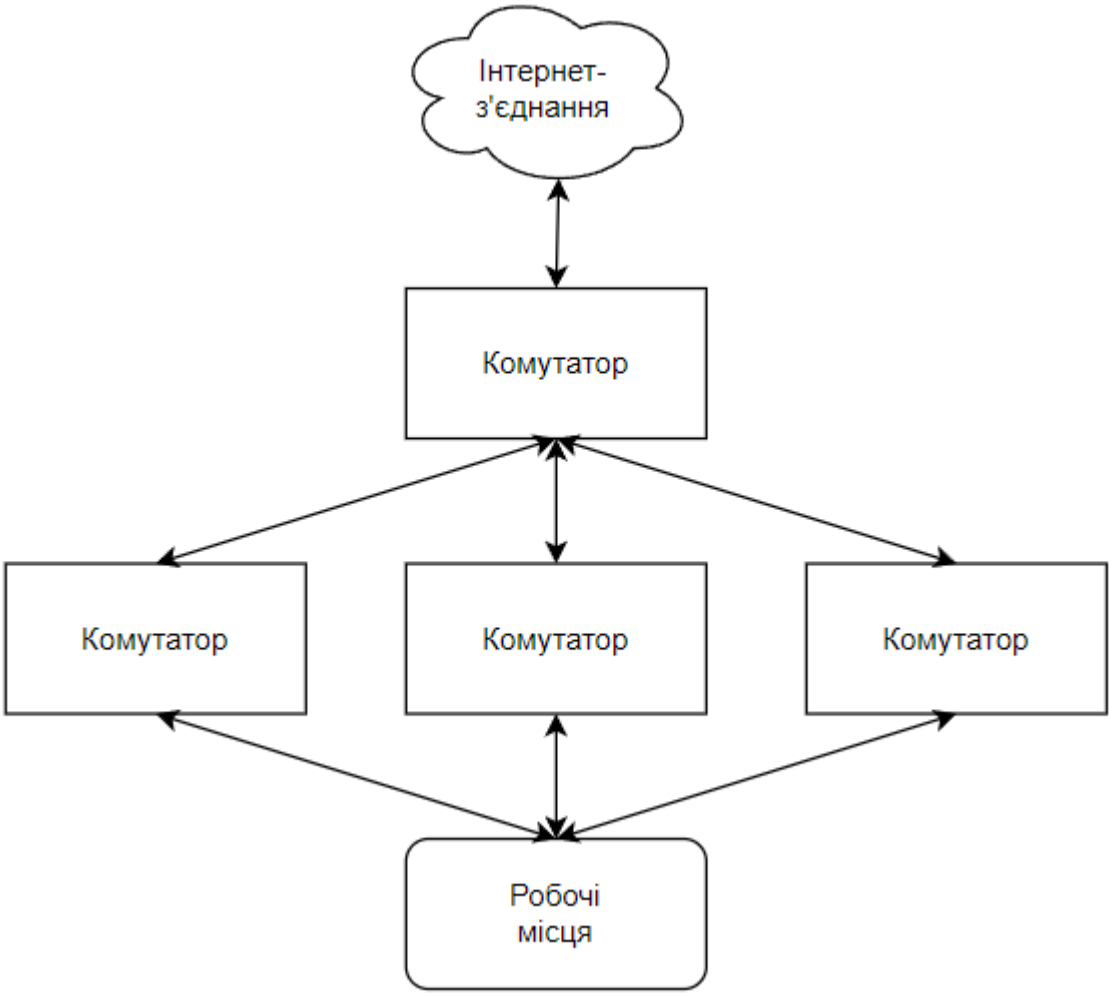

Рисунок 2.7 – структурна схема вузлу корпоративної мережі для порівняння

При достатньо рідкому проведенні операції моніторингу на дані 4 пристрої, збільшувалося навантаження на мережу, що відображалося на пропускній здатності і доводилося проводити дану операцію в обідню перерву або в неробочий час. Моніторинг по своїй суті – достатньо громіздка операція, в порівнянні з класичною командою ping, оскільки представляє собою генерацію в мережу TCP-трафіку з заданими параметрами та порівнянні відправленого та отриманого результатів. Проведення даної операції впливає на показник QoS (якість послуг). За результатами синтетичних тестів, проведених в періоди моніторингу на даному вузлі мережі, в які входили перевірка швидкості з'єднання, затримка та доступність вузлів, було виявлено в середньому: зниження швидкості на 6%, збільшення затримки з 3 до 11 мс, періодична втрата інтернет-з'єднання на певних підключеннях. При почерговому моніторингу, показники зменшились не настільки сильно: 0,5-1% втрати у швидкості, затримка збільшилася з 3 до 4 мс, або залишилася незмінною, а втрат інтернет-з'єднання не спостерігалось. Необхідність в проведенні операції моніторингу в даній мережі представлена в більшій мірі як виняток, в той час, коли в запропонованій мережі для виконання проактивного методу управління необхідний регулярний моніторинг.

Отримуємо залежність у витратах трафіку від кількості пристроїв на одночасному моніторингу. При моніторингу лише одного пристрою, втратою пропускної здатності можна знехтувати, проте, для проведення розрахунків узагальнимо та визначмо процентний показник втрати пропускної здатності при одному пристрої в діапазоні від 0,4 до 0,8%, оскільки він залежить від самого пристрою, проте в розрахунках будемо використовувати середній показник в 0,6%. Розподілення трафіку між користувачами, задачами та пріоритезацію опустимо, визначивши всю витрачену на них пропускну здатність корисною. Щоб розрахувати корисну пропускну здатність, необхідно відняти від заданої швидкості інтернет-з'єднання V_i частину, яка витрачається на моніторинг та сигнали управління, виражена як $V_i(0,006*n)$ та поділити отримане значення на задану швидкість. Отримуємо формулу 2.8:

$$Q = \frac{Vi - Vi(0{,}006 * n)}{Vi}, \text{ де} \quad (2.8)$$

Q – коефіцієнт корисної пропускної здатності, V_i – швидкість інтернет-з'єднання, n – кількість пристроїв, приймаючих участь в моніторингу.

Таким чином, при швидкості інтернет-з'єднання в 500 Мбіт/с та наявності 10 пристроїв, отримуємо коефіцієнт, який дорівнює 0,94. Втрата 6% при наявності всього 10 пристроїв є недопустимою для мережі міського масштабу, де їх кількість може і повинна бути більшою, особливо, коли є необхідність в завантаженні великих об'ємів даних, яка не допускає зволікань. Саме тому необхідно використовувати додаткову мережу для проведення описаних вище операцій проактивного управління комп'ютерною мережею.

Вибір методу управління комп'ютерною мережею

Описавши методи управління, їх переваги та недоліки між собою та взагалі, слід обрати напрямок, в якому буде будуватися концепція управління. Як зазначалося раніше, жодний з описаних методів не претендує на використання як єдино вірного рішення. Єдина можлива практика – гібридне комбінування цих методів з вичерпною кількістю переваг з кожного.

Запропонований варіант включає в себе велику комп'ютерну мережу міста, умовно поділену на підмережі для спрощення управління та при реалізації IPv6 та стандарту зв'язку 5G. Як вже вказувалося раніше, для покращення практики управління мережею, необхідно впроваджувати гібридний метод управління. Реалізація запропонованого варіанту зображена на рисунку 2.9:

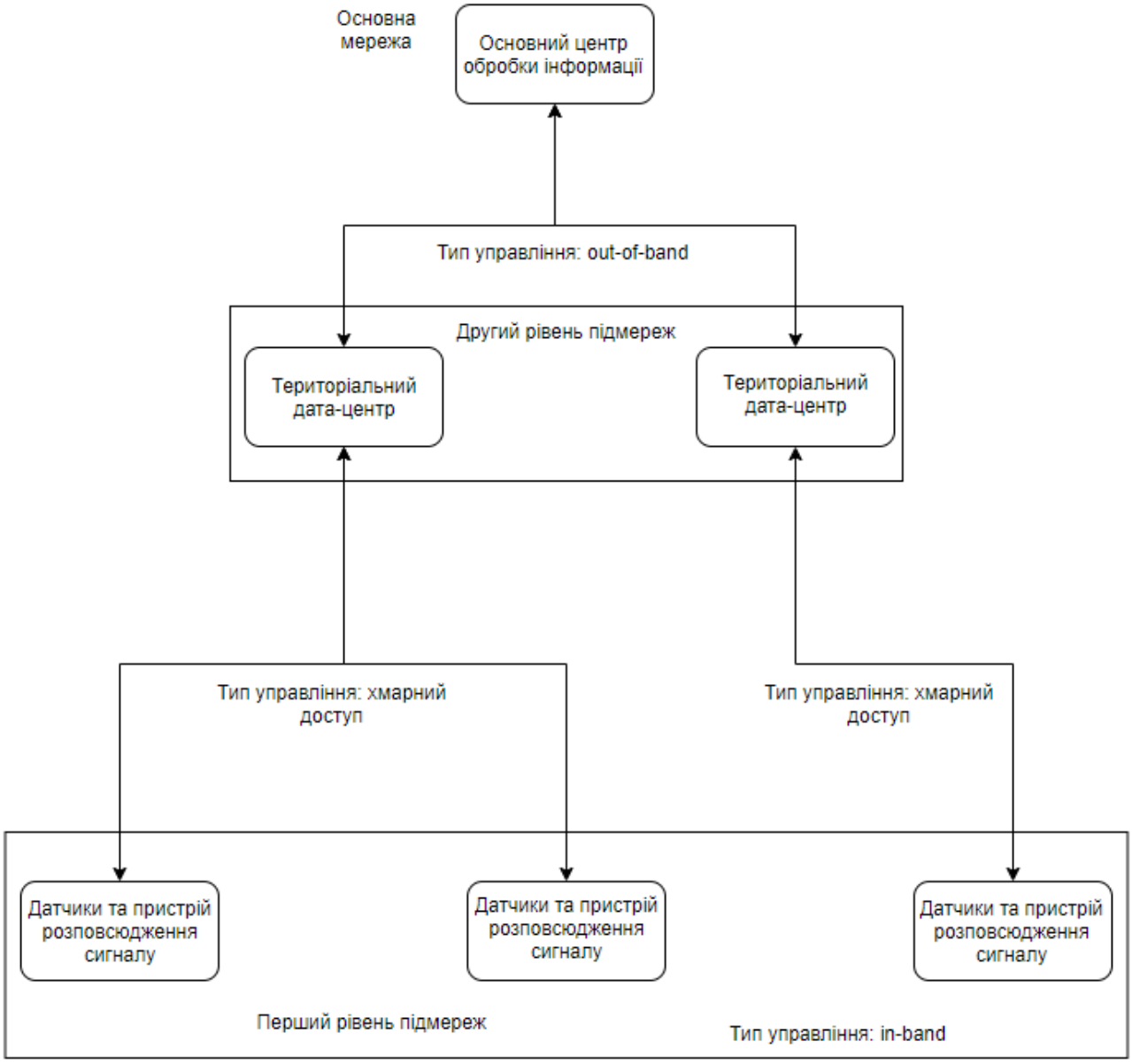

Рис. 2.9 – загальний принцип управління запропонованою мережею

На першому рівні підмереж знаходяться датчики та пристрої розповсюдження сигналу. Управління датчиками зазвичай виконується через один єдиний пристрій, а в самих датчиках немає додаткових інтерфейсів для управління, тому безпосередньо управління ними виконується за методом in-band, тобто тими самими каналами, що і весь трафік.

Територіальний дата-центр представляє собою місце збору інформації з датчиків, резервних копій конфігурацій, а також точку, з якої проводиться

моніторинг обладнання на даному рівні та нижче. Управління першою підмережою реалізується за допомогою хмарного доступу. Як правило, доступ надається саме до веб-інтерфейсів шлюзів, з яких розповсюджується сигнал на датчики, та через який створюються всі їх конфігурації.

Основним вузлом мережі вважається центр обробки інформації. В ньому, на запит користувачів чи органів влади, проводиться аналіз зібраних з датчиків даних. Звідси виконується управління над підмережою другого рівня використовуючи метод out-of-band. Оскільки в даному випадку існує необхідність у завантаженні великих об’ємів медіа-даних, управління необхідно відвести на інший канал.

2.4 Висновки за розділом

Проаналізувавши існуючі рішення, втілені та можливі у сфері мережевих технологій та телекомунікацій, а також інтернету речей та концепції «Розумне місто», були обрані найкращі практики до втілення. Запропонований варіант по управлінню комп’ютерною мережею втілює в собі рішення по створенню найбільш продуктивної мережі, пристосованої до втілення новітніх технологій.

Отримане рішення має перспективу подальшого покращення способом втілення технологій та рішень, які досі не набули популярності та повсюдного втілення через ряд обмежень. Подальше дослідження передбачає втілення в проект на основі SD-WAN технологій 5G та IPv6 в якості вже втілених в реальність практик.

Основною перевагою запропонованого рішення є можливість втілення в будь-якій мережі в якості універсального технічного рішення. Проект вирішує важливі питання по управлінню комп’ютерною мережею в практиках, де певні операції не вважаються необхідними. Основним недоліком в реалізації можуть бути проблеми у втіленні даного рішення через певні зауваження, котрі не описані

в проекті, які виникли при первинному проектуванні мережі та використовуються досі.

Всі теоретичні обґрунтування та висновки повинні бути в подальшому перевірені шляхом практичного втілення в існуючі моделі управління комп'ютерною мережею та їх об'єктивному порівнянні в реальних умовах.

3. МОДЕЛЮВАННЯ

3.1 Опис середи моделювання

Для моделювання був обраний програмний пакет Cisco Packet Tracer v.7.3.0.0838. Даний вибір обумовлений доволі широким набором мережевого обладнання для моделювання, наявності IoT пристроїв та можливістю моделювати певні мережеві сценарії.

3.2 Моделювання комп’ютерної мережі міської інфраструктури

Для моделювання пропонується розглянути модель розумного міста з розподіленням на умовні підмережі з метою спрощення налаштування та подальшого управління готовою мережею. Почати необхідно з першого рівня підмереж, в якому присутні датчики та пристрій розповсюдження сигналу. На даному рівні будуть присутні три варіанти комбінацій пристроїв IoT: сигналізація, освітлення, датчик руху та камера відеоспостереження для громадського закладу; сховище з датчиками вогню та рівнем води, а також протипожежні оприскувачі та відкачка води; паркінг, двері до якого відчиняються за наявності вуглекислого газу від автомобіля. Перелік пристроїв та їх умовне положення зображені на рисунку 3.1:

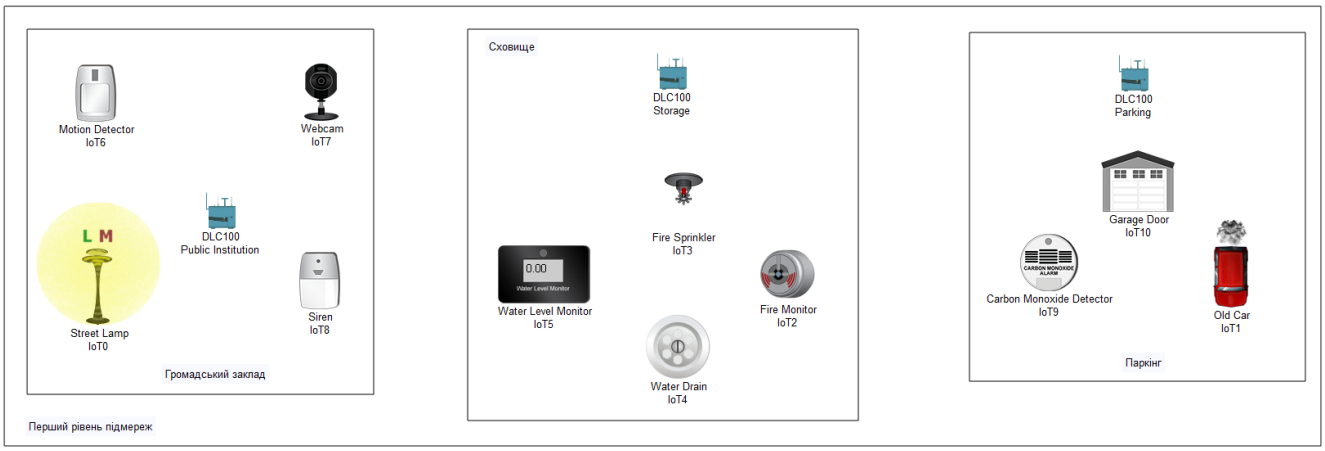

Рисунок 3.1 – перший рівень підмереж

Налаштуємо мережу в громадському закладі. Необхідно задати SSID та пароль на мережі шлюзу, що зображено на рисунку 3.2

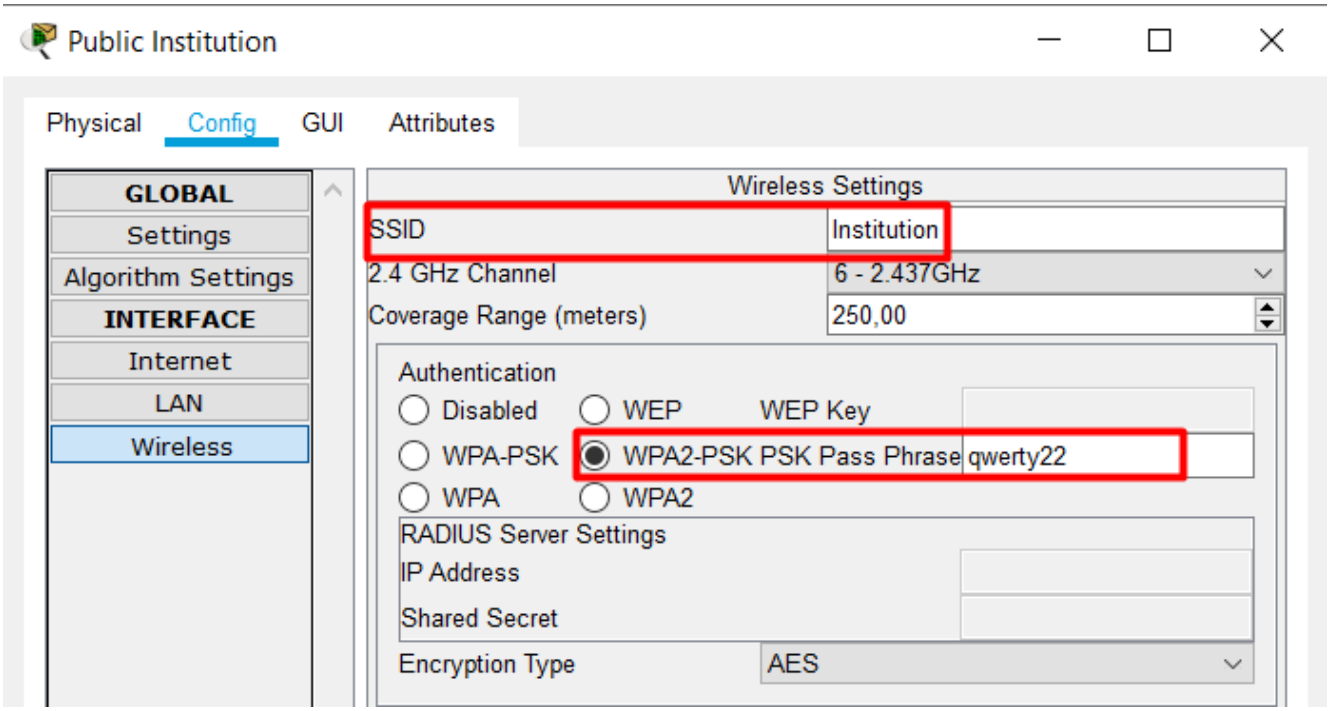

Рисунок 3.2 – налаштування бездротової мережі

Далі слід підключити всі IoT пристрої до даної мережі, обравши необхідний мережевий адаптер (PT-IOT-NM-1W) на кожному пристрої, що зображено на рисунку 3.3.

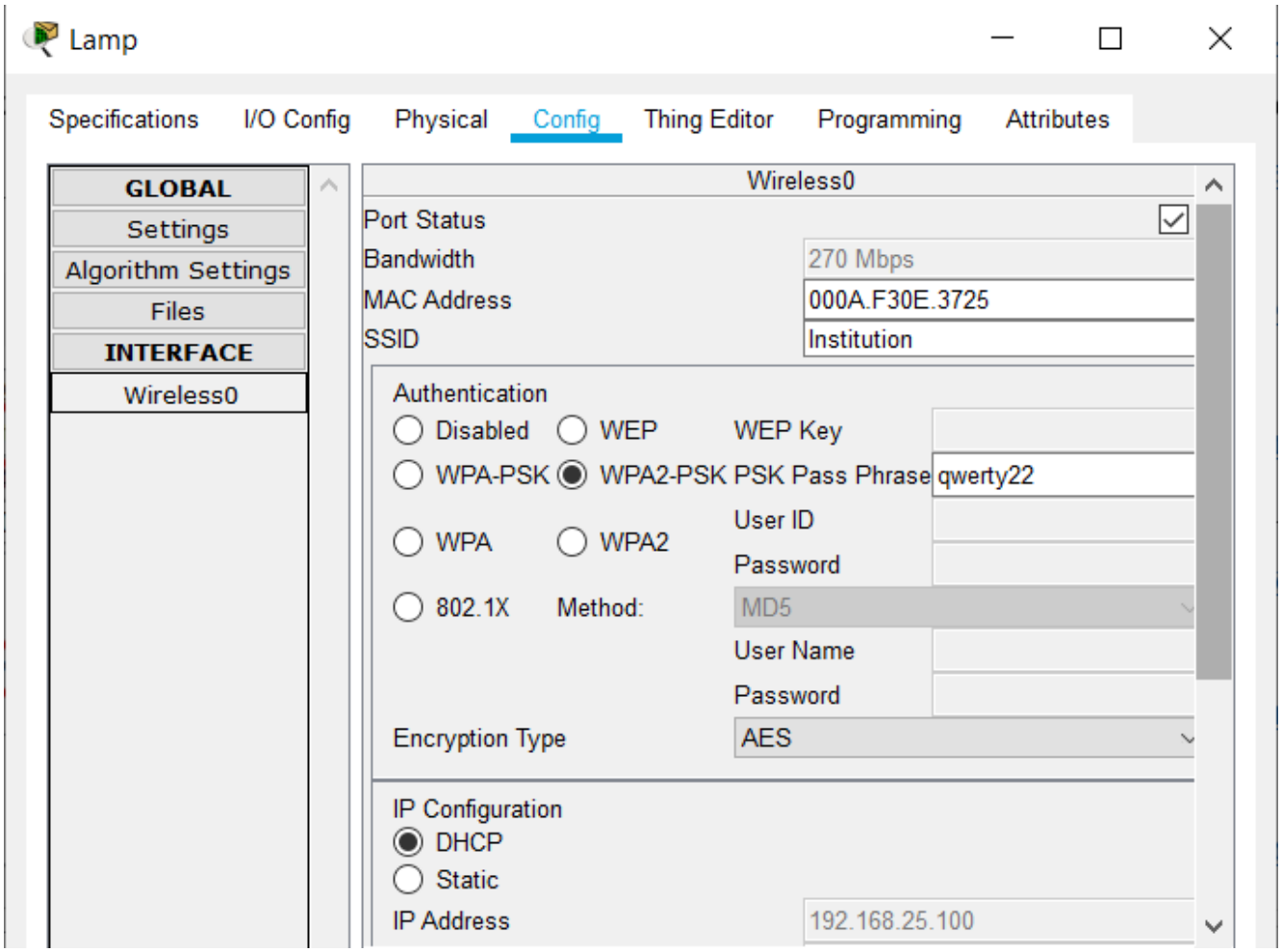

Рисунок 3.3 – підключення IoT пристроїв до мережі

Далі слід виконати підключення для інших пристроїв таким самим чином. Отримуємо готову мережу громадського закладу, зображену на рисунку 3.4:

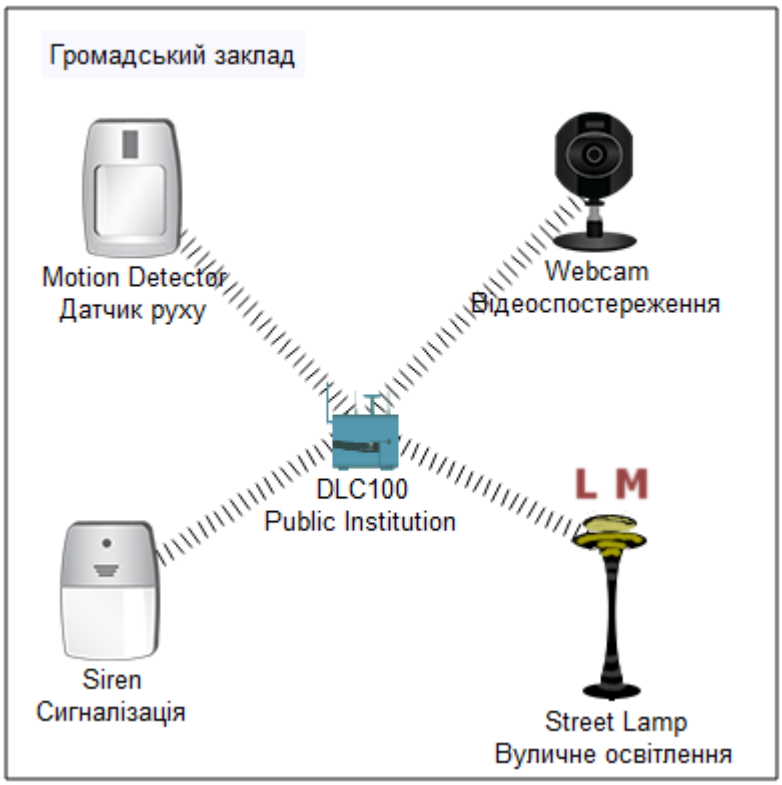

Рисунок 3.4 – мережа громадського закладу

Далі налаштуємо так само мережу сховища та паркінгу, змінивши на бездротових маршрутизаторах SSID та пароль, мережі котрих зображені на рисунку 3.5:

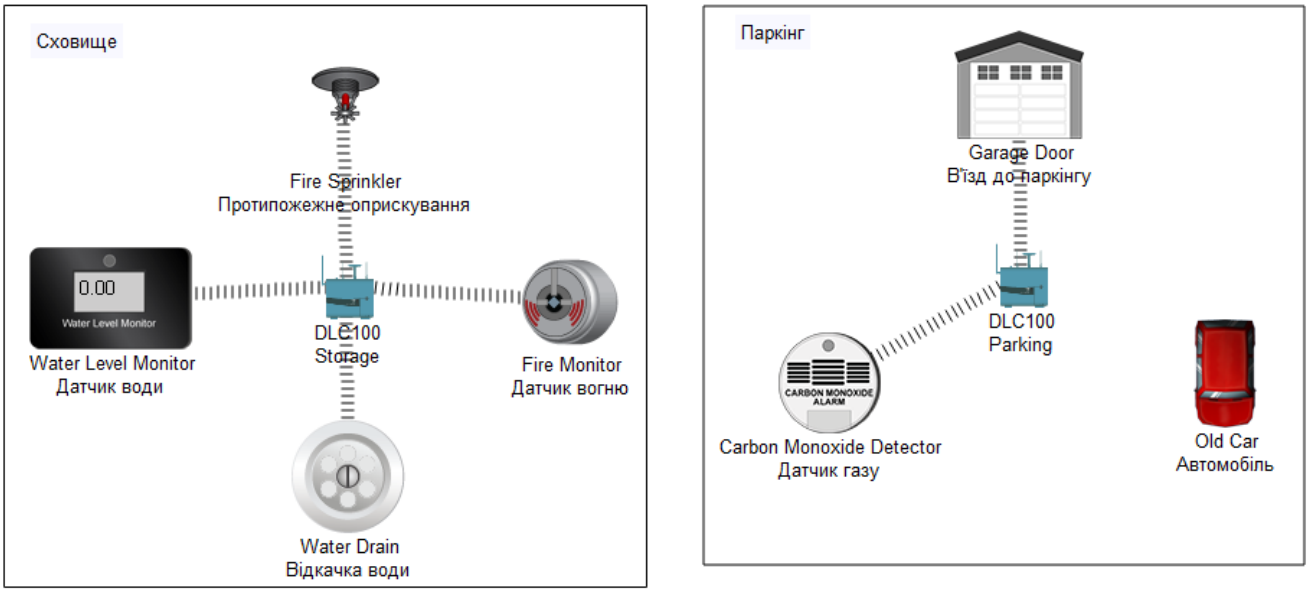

Рисунок 3.5 – мережі сховища та паркінгу

Управління пристроями відбувається з другого рівня підмереж, а, безпосередньо на першому рівні, управління датчиками відбувається через той самий канал зв’язку, по якому передаються всі дані, тобто маємо метод управління in-band.

Далі слід налаштувати другий рівень підмереж, з якого буде відбуватися управління першим. Реалізація через територіальні центри зручна розподіленням обов’язків не тільки умовним діленням на підмережі, а й створення декількох територіальних центрів обслуговування, щоб не накопичувати навантаження над всіма пристроями в рамках одного великого центру. Відносно невелика кількість пристроїв, за які відповідальний кожний центр допомагає зосередити увагу на моніторингу та в перспективі плину часу вивчити поведінкові особливості пристроїв у своєму регіоні, що допоможе зауважити виняткові випадки ще до моменту їх виникнення.

Важливими вузлами в рамках одного територіального центру є персональний комп’ютер, який виступає в ролі пристрою керування та моніторингу за мережею першого рівня, а також сервер FTP, на якому зберігаються резервні копії кожного пристрою та мережевий журнал, куди заносяться всі зміни в мережі з моменту її впровадження. Також можливе збереження певної кількості зібраної з датчиків інформації. Приклад мережі зображений на рисунку 3.6, а приклад доступу до FTP – на рисунку 3.7:

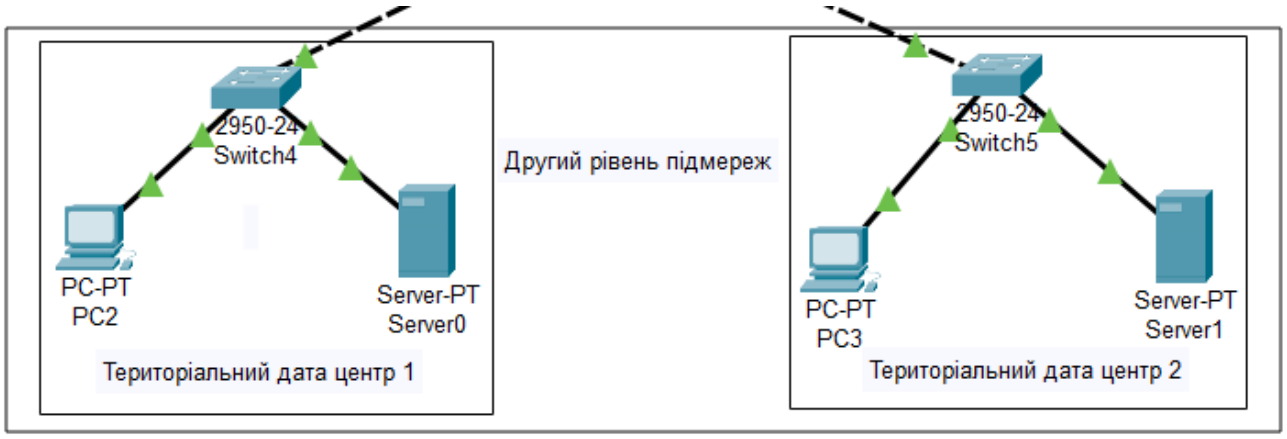

Рисунок 3.6 – другий рівень підмереж

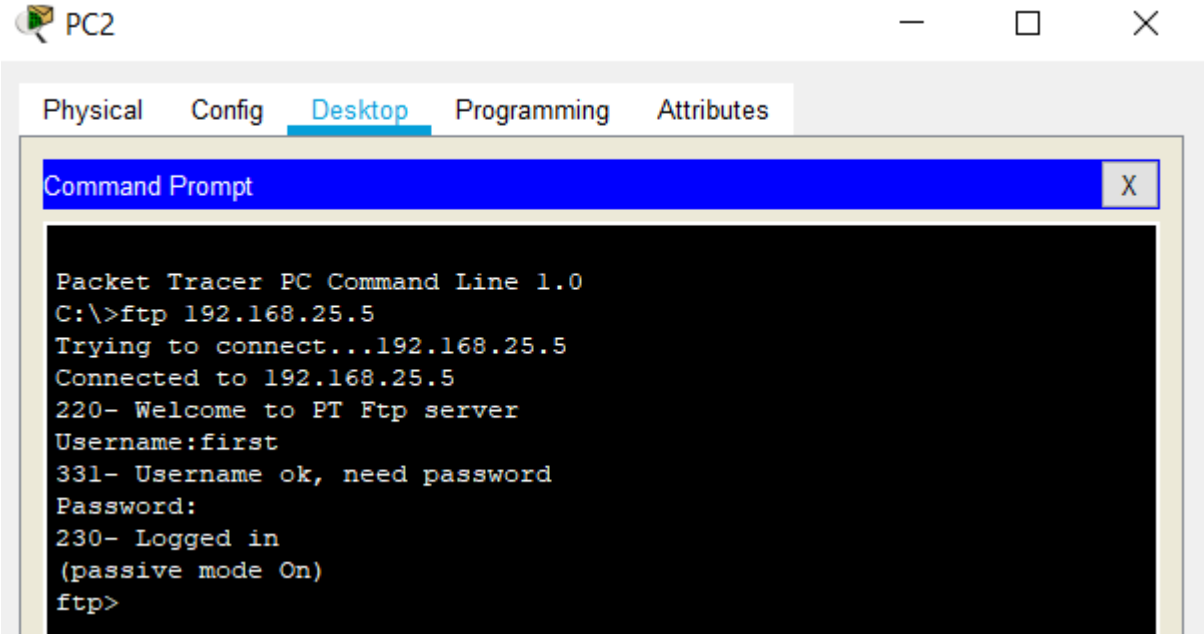

Рисунок 3.7 – приклад доступу до FTP

Управління першим рівнем відбувається за допомогою хмарних технологій. Налаштування лише одного такого територіального центру не є гарним рішенням, адже в масштабах реальної міської інфраструктури кількість датчиків та пристроїв IoT може налічувати понад 100000, тому необхідне розподілення обсягу за територіальним критерієм. В запропонованій моделі управління за громадський заклад відповідає перший територіальний центр, а за сховище та паркінг – другий. На практиці, підконтрольних елементів буде значно більше. Підключення першого рівня підмереж до другого зображено на рисунку 3.8:

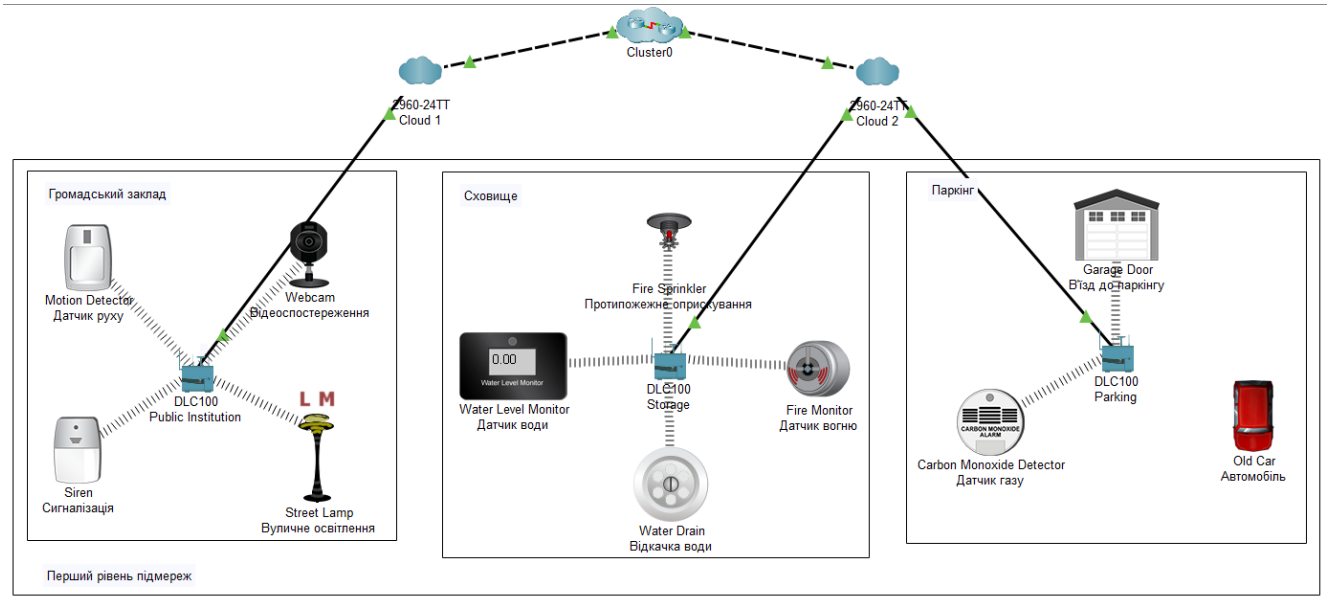

Рисунок 3.8 – хмарне управління першим рівнем підмереж

Тепер, маючи доступ до першого рівня підмереж, можна налаштувати сценарії роботи датчиків на кожному з закладів першого рівня. Для налаштування датчиків громадського закладу, необхідно зайти в IoT монітор, який доступний з персонального комп'ютера першого територіального центру. Монітор управління зображений на рисунку 3.9:

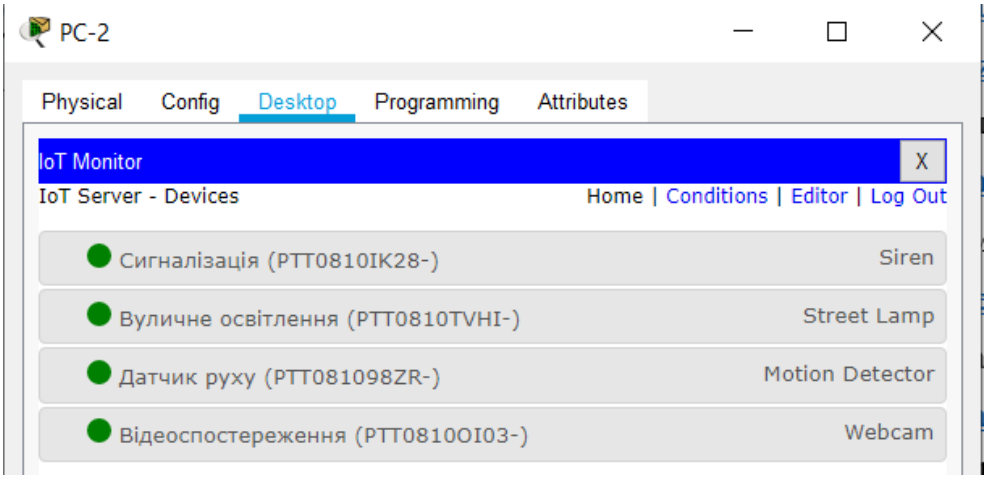

Рисунок 3.9 – Список IoT пристроїв у громадському закладі

Далі необхідно створити сценарії роботи для кожного пристрою. В даному випадку вуличне освітлення буде самодостатнім: освітлення буде автоматично вмикатись при недостатній освітленості. Також можливе його вимкнення у випадку відсутності руху, який фіксується вбудованим датчиком, проте, оскільки це громадський заклад, освітлення для відвідувачів повинне бути постійним. Сигналізація, датчик руху та камера відеоспостереження працюють разом: у випадку фіксації руху, коли заклад вже зачинений, вмикається сигналізація та камера, яка починає запис і одразу відправляє його. Сценарій роботи сигналізації зображений на рисунку 3.10:

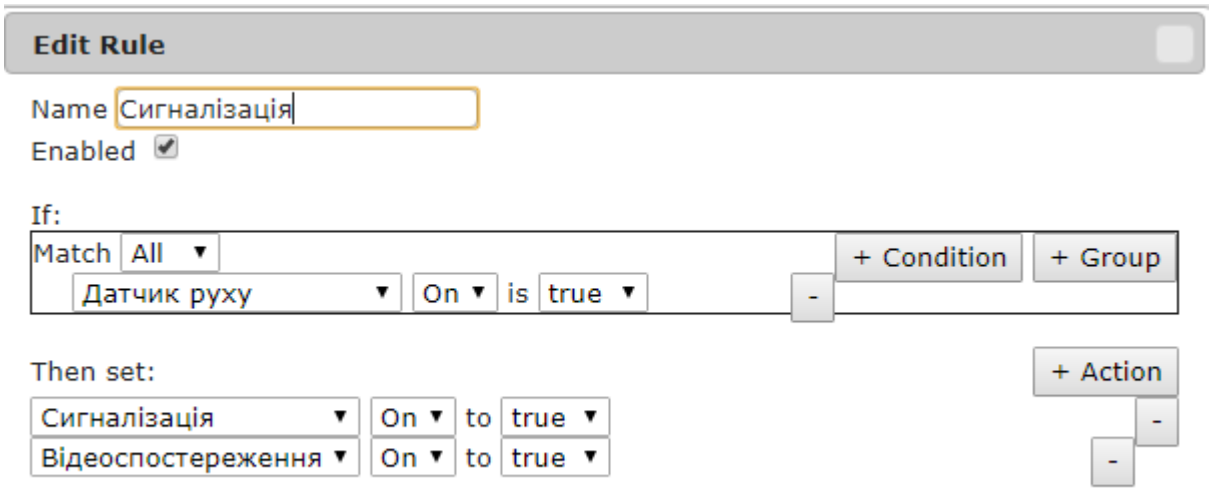

Рисунок 3.10 – сценарій роботи сигналізації громадського закладу

Налаштування двох інших мереж будуть відбуватися з комп’ютера другого територіального центру. Для сховища сценарій буде наступним: у випадку виникнення пожежі, датчик вогню фіксує присутність полум’я і вмикає протипожежний оприскувач, а щоб приміщення не стало затопленим, працює датчик рівню води, який вмикає відкачку, коли рівень води досягне певної відмітки. Протипожежний сценарій та сценарій на випадок затоплення зображені на рисунках 3.11 та 3.12 відповідно.

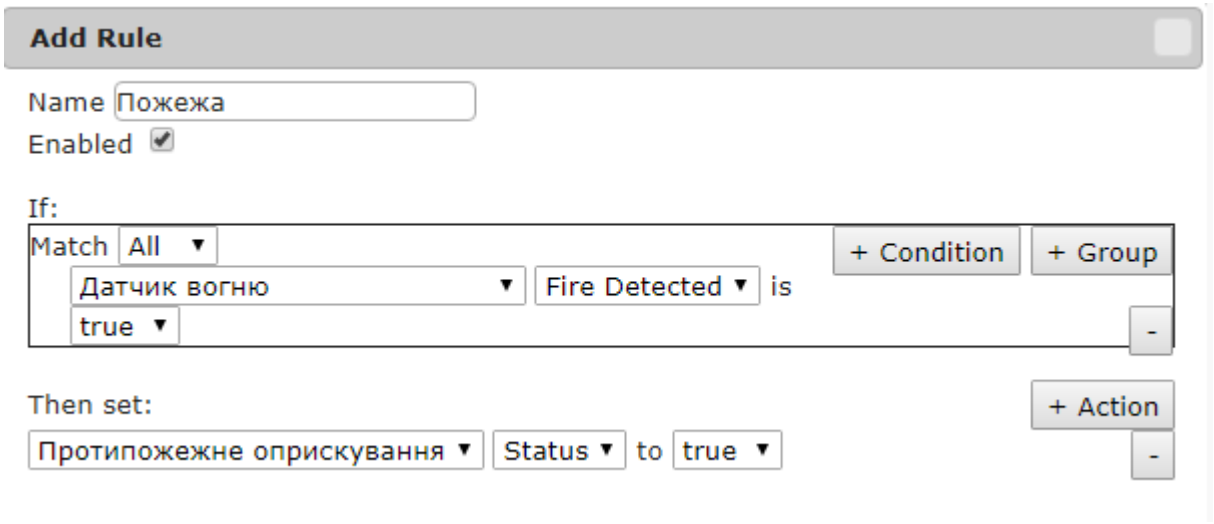

Рисунок 3.11 – протипожежний сценарій сховища

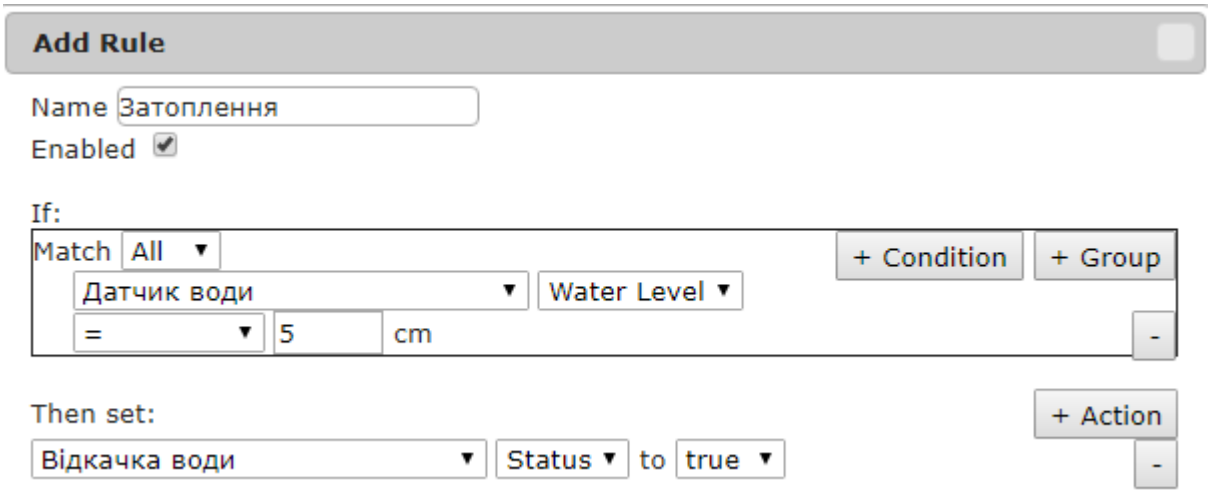

Рисунок 3.12 – сценарій на випадок затоплення сховища

Система паркінгу буде працювати наступним чином: датчик вуглекислого газу буде фіксувати приїзд автомобілю і дасть сигнал на відчинення гаражних дверей до паркінгу і до моменту, коли автомобіль під'їде до дверей, вони вже будуть відчинені. Сценарій для паркінгу зображений на рисунку 3.13:

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Паркінг	Датчик газу Level > 10	Set В'їзд до паркінгу On to true
Edit Remove	Yes	Закрити паркінг	Датчик газу Level = 0	Set В'їзд до паркінгу On to false

Рисунок 3.13 – сценарій для паркінгу

Далі необхідно створити основну мережу, яка керує другим рівнем методом управління out-of-band. Використання консольного підключення не характерно для великої віддаленості вузлів мережі. Саме тому його використання обумовлене територіальними масштабами самого міста. Кожний з умовних районів, в яких перебувають підмережі першого рівня, знаходяться на довільному віддалені від територіального центру, тобто другого рівня підмереж, саме тому, обраний, для даних потреб, метод управління не залежить від віддаленості і працює з єдиною умовою – наявність інтернет-з'єднання. Віддалення між другим рівнем підмереж та основною мережею не є суттєвим (наприклад невелике віддалення між будівлями, або використання різних поверхів в межах однієї будівлі) і має можливості та переваги використання консольного типу управління. Серед основних: можливість доступу навіть за невдалого завантаження мережевого обладнання або за відсутності інтернет-з'єднання; усунення відмов через несправність прошивки нещодавно встановленого програмного забезпечення; оновлення прошивки тощо.

В ній будуть присутні звичайні для мереж корпоративного типу комп'ютер, сервер, мережеве обладнання, проте для простоти моделювання вона буде втілена одним персональним комп'ютером, одним сервером під різні потреби та одним ноутбуком, який буде використовуватися для консольного управління другим рівнем підмереж. Комп'ютер та сервер будуть мати доступ для другого рівня підмереж з метою отримання певної інформації з датчиків на запит користувача. Приклад основної мережі представлений на рисунку 3.14:

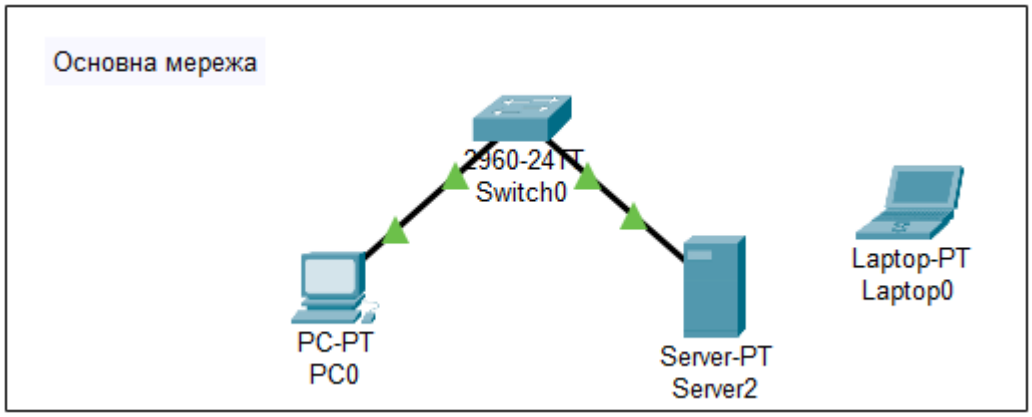

Рисунок 3.14 – пристрої основної мережі

Після налаштування мережі, необхідно створити консольне підключення. Використання для даних потреб ноутбуку обумовлене його портативністю, адже персональний комп’ютер закріплюється за певним територіальним положенням і за рахунок великої кількості периферії не є зручним для пересування. В ролі посередника між пристроями та ноутбуком буде консольний сервер. Кожний критично важливий мережевий пристрій, який можливо підключити до даного серверу, повинен бути підключеним. Переваги використання консольного серверу визначаються при використанні будь-якого методу управління, проте саме в out-of-band він розкривається в повній мірі. Після з’єднання консольним кабелем відповідного порту консольного серверу з портом RS-232 на ноутбуку маємо доступ до консольного управління та налаштування. Приклад консольного доступу приведено на рисунку 3.15:

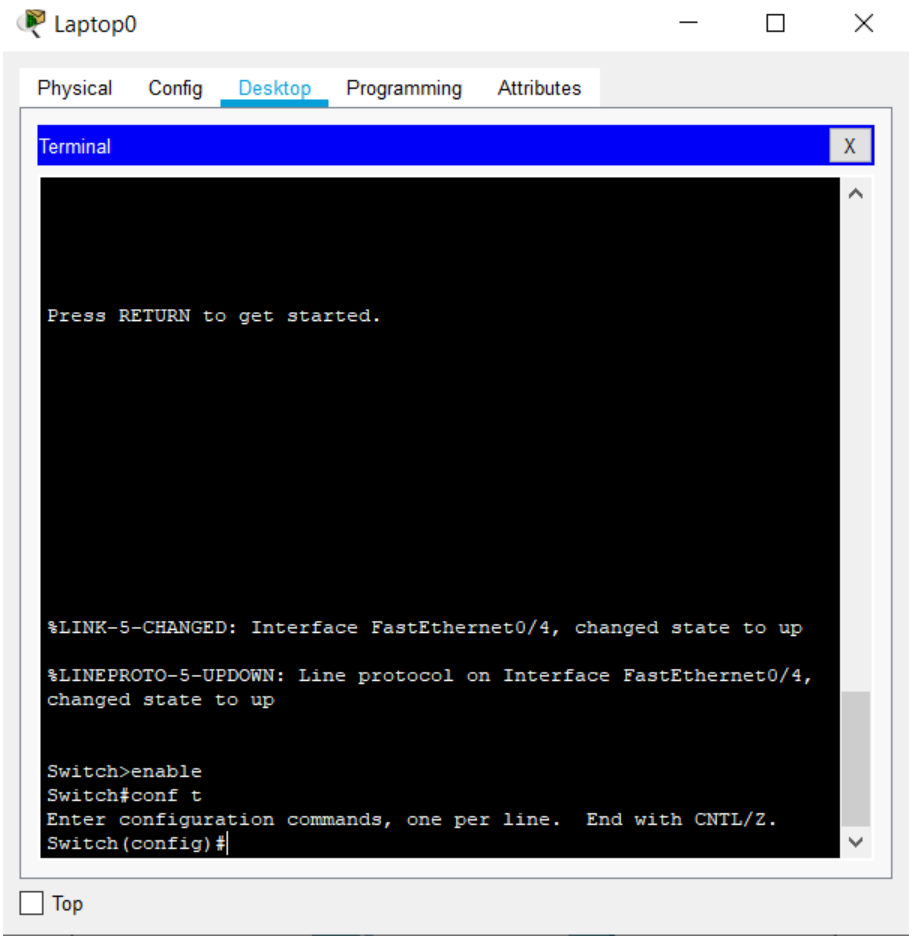

Рисунок 3.15 – приклад доступу до комутатору через консольне з’єднання

Після виконання даних операцій отримуємо готову мережу, яка приймає дані з підмережі другого рівня та здатна керувати нею, не використовуючи канали зв’язку для користувальницького трафіку. З’єднання другого рівня підмереж з основною мережею приведено на рисунку 3.16:

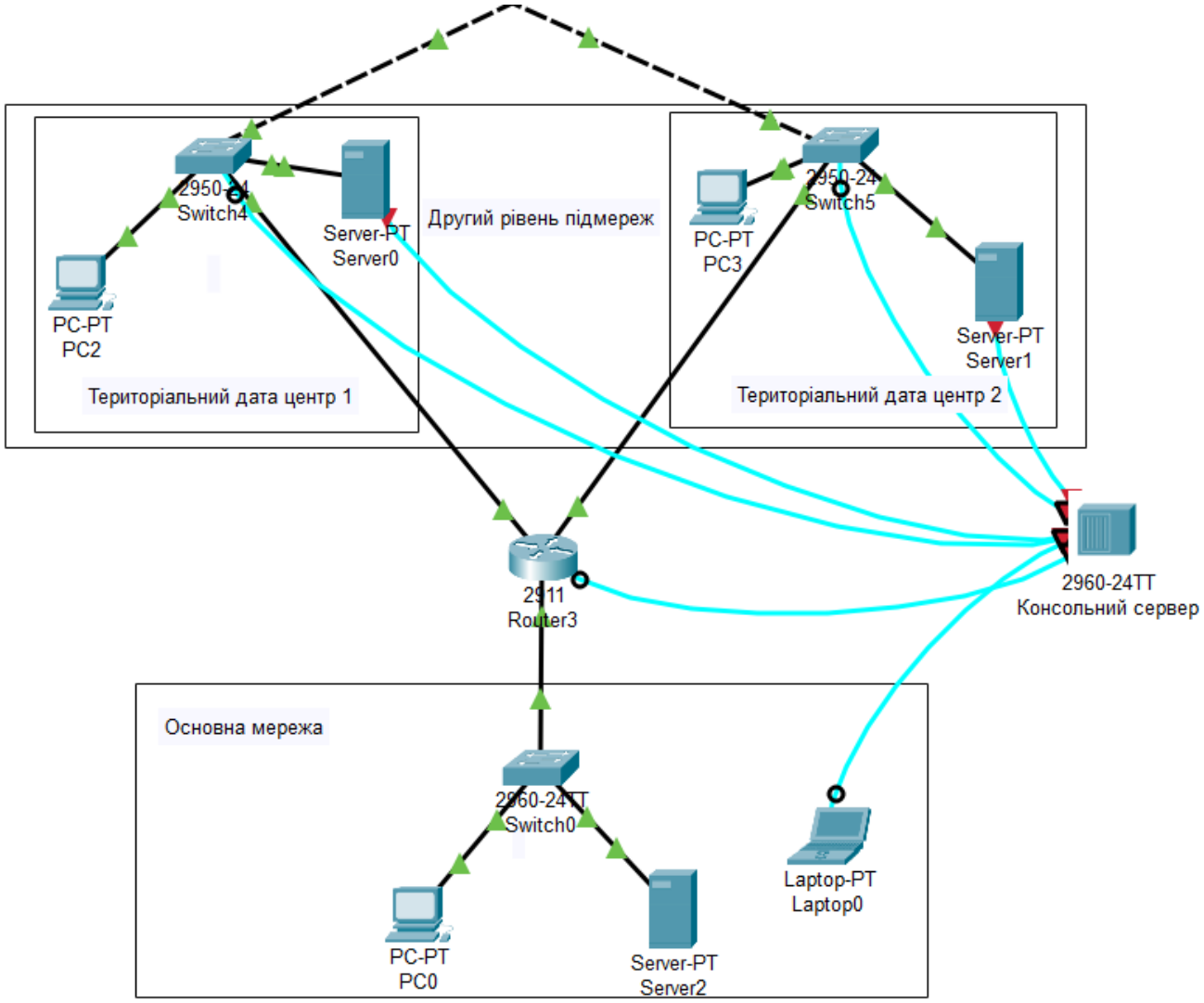

Рисунок 3.16 – з’єднання другого рівня підмереж з основною мережею через консольний сервер

3.3 Висновки за розділом

В даному розділі була представлена модель функціонування тестової мережі з використанням гібридного методу управління на прикладі мережі концепції «Розумне місто». Були промодельовані всі описані методи управління та налагоджений зв’язок між ними та перехід з одного методу на інший.

За результатами моделювання можна визначити переваги використання такої концепції управління комп’ютерною мережею. Умовний поділ на підмережі робить систему стійкою до масштабування в будь-яких вузлах інфраструктури, що позитивно відображається на подальшому розвитку самого міста та його цифровізації. Пропускна здатність в критично важливих вузлах забезпечена, а там, де немає необхідності у великих швидкостях (наприклад консольне підключення) зберігається баланс мінімально необхідної пропускної здатності. Також дана система націлена на підвищення рівня продуктивності мережі, що доводять результати моделювання.

Щоб підвищити якість результату моделювання необхідно:

1. Виконання моделювання в іншому середовищі, де можливе максимально повне розкриття функціонування методу управління out-of-band та втілення в повній мірі реального практичного функціоналу.
2. Підвищення деталізації певних вузлів мережі для повної реалізації масштабу.
3. Проаналізувати існуючі мережі, які використовують схожі тенденції по розподіленню функціоналу та використовують пристрої IoT, щоб оцінити реально можливий обсяг закладів, за які буде відповідальний один територіальний центр.

Концепція підлягає вдосконаленню шляхом тестового втілення та порівняння з існуючими методами та операціями по управлінню комп’ютерною мережею. В подальшому можлива заміна певних аспектів управління шляхом впровадження технології програмно-орієнтованих мереж міського типу SDN.

ВИСНОВКИ

В даній науковій роботі був запропонований комплекс операцій, методів та підходів по управлінню комп'ютерної мережі міської інфраструктури на основі концепції проекту «Розумне місто».

Був проведений аналіз джерел інформації в різних галузях, пов'язаних з предметом дослідження в рамках його реалізації та необхідності. Проаналізувавши існуючі рішення, втілені та можливі у сфері мережевих технологій та телекомунікацій, а також інтернету речей та концепції «Розумне місто», були обрані найкращі практики до втілення. Запропонований варіант по управлінню комп'ютерною мережею втілює в собі рішення по створенню найбільш продуктивної мережі, пристосованої до втілення новітніх технологій.

Обрані технічні рішення для реалізації всіх функцій та вузлів проекту були розглянуті більш детально з метою виявлення найкращої синергії у втіленні. Також були розглянуті перспективні рішення, які досі не набули належної популярності та попиту, але в подальшому повинні використовуватися повсюдно.

В запропонованій моделі по управлінню неможливе використання лише одної з досліджених моделей управління, саме тому використовувався загальний комплекс рішень, який поєднував в собі необхідні якості.

Були описані три методи управління комп'ютерною мережею: in-band, out-of-band та хмарний доступ. Кожен з них був втілений в загальну модель функціонування та управління та гармонічно поєднаний з іншими. Використання кожного методу описано для певних задач, проте на практиці не обмежується лише ними.

Загальну модель мережі було запропоновано поділити на умовні підмережі, що в кількісному показнику значно економить затрачений на впровадження та

підтримку працездатності інфраструктури, а в якісному показнику дозволяє більш явно розподілити функціональні обов’язки в межах кожної з підмереж та, за необхідності, встановити бажані права та пріоритети.

При моделюванні було розглянуто три типи підмереж та методів управління: на першому рівні громадський заклад, сховище та паркінг, складові яких це датчики та різноманітні розумні пристрої з шлюзом на кожну підмережу, в якій управління втілено методом in-band; на другому рівні розташовані територіальні центри, які керують першим за допомогою хмарного доступу; третій рівень підмереж представляє собою головний офіс, з якого можливе управління територіальними центрами методом out-of-band.

Основною перевагою запропонованого рішення є можливість втілення в будь-якій мережі в якості універсального технічного рішення. Використання даної моделі управління здатне зменшити втрату пропускної здатності при виконанні операції моніторингу на кожні 10 пристроїв на 6%.

Отримане рішення має перспективу подальшого покращення способом втілення технологій та рішень, які досі не набули популярності та повсюдного втілення через ряд обмежень. Подальше дослідження передбачає втілення в проект на основі SD-WAN технологій 5G та IPv6 в якості вже втілених в реальність практик.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Четверта промислова революція [Електронний ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Четвертая_промышленная_революция_(Industry_Индустрия_4.0)
2. Теорія рішень «розумного» міста та можливості її реалізації на базі єдиної муніципальної платформи [Електронний ресурс]. URL: https://hub.kyivstar.ua/news/teoriya-reshenij-umnogo-goroda-i-vozmozhnosti-ee-realizaczii-na-baze-edinoj-municzipalnoj-platformy/
3. Рейтинг «розумних» міст світу на 2017 рік [Електронний ресурс]. URL: https://tehnot.com/ua/sostavlen-rejting-umnyh-gorodov-mira/
4. Розумний дім – Wiki ТНТУ [Електронний ресурс]. URL: https://wiki.tntu.edu.ua/Розумний_дім
5. Прогнози урбанізації за даними ООН [Електронний ресурс]. URL: https://www.kommersant.ru/doc/3630399
6. Технології Winkhaus для розумних будинків [Електронний ресурс]. URL: https://okna.ua/ua/library/winkhaus-rozumnyy-budynok
7. IPv6 adoption by Google [Електронний ресурс]. URL: https://www.google.com/intl/en/ipv6/statistics.html
8. Що таке і навіщо потрібен IPv6 [Електронний ресурс]. URL: https://droider.ru/post/chto-takoe-i-zachem-nuzhen-ipv6-razbor-09-06-2021/
9. 5G, патенти, майбутнє [Електронний ресурс]. URL: https://vc.ru/future/106836-5g-statistika-patenty-budushchee
10. Коли буде 5G в Україні і чим краще 5G за 4G мережу [Електронний ресурс]. URL: https://ktc.ua/blog/koli_5g_bude_v_ukrayini_i_chim_5g_krashhe_za_4g_merezhu.html

11. Керування комп'ютерною мережею – Wiki [Електронний ресурс]. URL: https://ru.wikipedia.org/wiki/Управление_компьютерной_сетью
12. Основні функції керування комп'ютерною мережею [Електронний ресурс]. URL: https://eopearhiiv.edu.ee/e-kursused/eucip/haldus_vk/611___.html
13. Засоби керування корпоративними мережами та застосунками [Електронний ресурс]. URL: https://compress.ru/article.aspx?id=12065
14. Управління мережею передачі даних [Електронний ресурс]. URL: https://www.osp.ru/lan/2014/09/13042711
15. In-band management [Електронний ресурс]. URL: https://library.netapp.com/ecmdocs/ECMP12404965/html/GUID-CA995A42-1406-4F70-A1B6-1FE8BC0DC32E.html
16. Out-of-band management networks [Електронний ресурс]. URL: https://www.networkers-online.com/blog/2010/08/out-of-band-management-networks/
17. Out-of-band management [Електронний ресурс]. URL: https://www.wti.com/pages/out-of-band-management-oobm
18. In-band and out-of-band Network Management: Detailed Comparison [Електронний ресурс]. URL: https://networkinterview.com/in-band-and-out-of-band-network-management-detailed-comparison/
19. Cisco Meraki Solutions [Електронний ресурс]. URL: https://www.facebook.com/ciscomerakiindia/photos/a.181802004509547 1/2436022769961859/?type=3&theater
20. Технологія SD-WAN – «нервова система» цифрового підприємства майбутнього [Електронний ресурс]. URL: https://www.2test.ru/publications/Tekhnologiya-SD-WAN-nervnaya-sistema-tsifrovogo-predpriyatiya-budushchego.html
21. Рішення SD-WAN – короткий огляд Cisco SD-WAN [Електронний ресурс]. URL: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-07-enterprise-grade-wp-cte-en.html