ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
Кафедра Мобільних та відеоінформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Метод забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

(підпис) Сергій ЛИСЕНКО (Ім'я, ПРІЗВИЩЕ)

Виконав: здобувач вищої освіти
групи АРДМ-62
Сергій ЛИСЕНКО

Керівник: Любов БЕРКМАН

Рецензент: С. Прокопов

Київ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

Кафедра	Мобільних та відеоінформаційних технологій
Ступінь вищої освіти	Магістр
Спеціальність	172 Електронні комунікації та радіотехніка
Освітньо-професійна програма	Апаратура радіозв'язку, радіомовлення і телебачення

ЗАТВЕРДЖУЮ
Завідувачка кафедрою МВТ
_____ Наталія РУДЕНКО
« » _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лисенку Сергію Юрійовичу

1. Тема кваліфікаційної роботи: «Метод забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління»,
керівник кваліфікаційної роботи Любов БЕРКМАН, д.т.н., професор,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 15.10.2024 р. №320.

2. Строк подання кваліфікаційної роботи 25.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. 5G-мережі;
   2. Розумне Місто;
   3. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   1. Телекомунікаційна інфраструктура Розумного Міста;
   2. Мобільні мережі п'ятого покоління в інфраструктурі Розумного Міста;
   3. Методи забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням 5G;

5. Перелік ілюстративного матеріалу: презентація.

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	26.10.24	Викон.
2.	Телекомунікаційна інфраструктура Розумного Міста	29.10.24	Викон.
3.	Мобільні мережі п'ятого покоління в інфраструктурі Розумного Міста	01.12.24	Викон.
4.	Методи забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням 5G	02.11.24	Викон.
5.	Висновки, вступ, реферат	11.12.24	Викон.
6.	Розробка презентації	25.12.24	Викон.

Здобувач вищої освіти _____ Сергій ЛИСЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Любов БЕРКМАН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Лисенка Сергія Юрійовича

на тему: «Метод забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління»

Актуальність:

Актуальність теми обумовлена зростанням кількості підключених пристроїв та обсягів даних в інфраструктурі Розумного Міста, що створює значні виклики для забезпечення кібербезпеки. Мобільні мережі п'ятого покоління (5G) надають нові можливості для підвищення рівня захисту за рахунок розширених функцій мережевої безпеки, таких як сегментація трафіку, шифрування на рівні доступу та розподілене управління автентифікацією. Використання проактивного підходу до виявлення та реагування на загрози дозволяє ефективно захищати критичні сервіси міської інфраструктури та забезпечувати безперервність їхньої роботи.

Позитивні сторони:

1. Зміст магістерської роботи відповідає завданню. Її автор, показала високий рівень знань і ступінь підготовленості до майбутньої роботи за фахом.

2. Текст викладений грамотно, ясно, послідовно. Графічний матеріал оформлений якісно. Широко використовується сучасна науково-технічна література, включаючи англомовні видання.

Недоліки:

1. Уточнити вплив малих комірок (Small Cells) на підвищення ємності мережі, враховуючи необхідність щільного розгортання в густонаселених районах.

2. Рекомендується додати практичні рекомендації щодо впровадження заходів безпеки, зокрема використання ШІ для моніторингу кіберзагроз.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота заслуговує оцінку «відмінно», а здобувач Лисенко Сергій Юрійович заслуговує присвоєння кваліфікації: «Магістр з електронних комунікацій та радіотехніки».

Рецензент: к.т.н., доцент _____ Пристоть С.В

(науковий ступінь, вчене звання) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Лисенко С.Ю. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 172 Електронні комунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

на тему: Метод забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління

Кваліфікаційна робота і рецензія додаються.

В.о. директора ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Лисенко Сергій Юрійович показав гарну теоретичну та інженерну підготовку, уміння володіти технологіями нового покоління, вміло працювати з програмно-апаратними засобами мобільного зв'язку, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу Лисенка Сергія Юрійовича на оцінку «відмінно» та присвоїти йому кваліфікацію «Магістр з електронних комунікацій та радіотехніки».

Керівник кваліфікаційної роботи _____ Любов БЕРКМАН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

“ ” _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Лисенко С.Ю.
(прізвище та ініціали)

допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувачка кафедрою
Мобільних та відеоінформаційних технологій _____ Наталія РУДЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

“ ” _____ 2024 року

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 72 стор., 7 рис., 8 табл., 30 дж.

Мета роботи – дослідження методів забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління.

Об'єкт дослідження – процес взаємодії Розумного Міста і мереж п'ятого покоління.

Предмет дослідження – методи забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління.

Короткий зміст роботи: У першому розділі досліджено ключові компоненти та архітектуру телекомунікаційної інфраструктури розумного міста. Проаналізовано основні елементи, такі як інтелектуальне управління транспортом, розумні енергомережі та використання технологій IoT і великих даних. Наведено вимоги до інфраструктури, включаючи продуктивність, надійність і масштабованість, а також підкреслено роль технологій 5G і Wi-Fi 6.

Другий розділ присвячено архітектурним особливостям мобільних мереж 5G у розумному місті. Розглянуто ключові технології, зокрема нарізку мережі, Massive MIMO, Beamforming і Edge Computing. Визначено їхню роль в оптимізації ресурсів, підвищенні пропускної здатності та зниженні затримок. Порівняно характеристики мереж 4G та 5G, підтверджуючи переваги останньої для міської інфраструктури.

У третьому розділі розглянуто методи забезпечення кібербезпеки інфраструктури розумного міста на основі 5G. Проаналізовано основні загрози та запропоновано заходи захисту, такі як шифрування, багаторівнева автентифікація та моніторинг трафіку. Запропоновані методи охоплюють захист IoT, транспортних систем і конфіденційності даних, забезпечуючи надійність та стійкість міської інфраструктури.

КЛЮЧОВІ СЛОВА: РОЗУМНІ МІСТА, 5G, 4G, MASSIVE MIMO, BEAMFORMING І EDGE COMPUTING, IOT, ШИФРУВАННЯ, БАГАТОРІВНЕВА АВТЕНТИФІКАЦІЯ ТА МОНІТОРИНГ ТРАФІКУ.

ABSTRACT

Text part of the master's qualification work: 72 pages, 7 pictures, 8 table, 30 sources.

The purpose of the work is to study methods for ensuring cybersecurity in the Smart City infrastructure using fifth-generation mobile networks.

The object of the research is the process of interaction between the Smart City and fifth-generation networks.

The subject of the research is methods for ensuring cybersecurity in the Smart City infrastructure using fifth-generation mobile networks.

Summary of the work: The first section examines the key components and architecture of the telecommunications infrastructure of a smart city. The main elements, such as intelligent transport management, smart power grids and the use of IoT and big data technologies, are analyzed. The requirements for the infrastructure, including performance, reliability and scalability, are presented, and the role of 5G and Wi-Fi 6 technologies is emphasized.

The second section is devoted to the architectural features of 5G mobile networks in a smart city. Key technologies are considered, in particular, network slicing, Massive MIMO, Beamforming and Edge Computing. Their role in optimizing resources, increasing throughput and reducing delays is determined. The characteristics of 4G and 5G networks are compared, confirming the advantages of the latter for urban infrastructure.

The third section considers methods for ensuring cybersecurity of smart city infrastructure based on 5G. The main threats are analyzed and protection measures are proposed, such as encryption, multi-level authentication and traffic monitoring. The proposed methods cover the protection of IoT, transport systems and data confidentiality, ensuring the reliability and resilience of urban infrastructure.

KEYWORDS: SMART CITIES, 5G, 4G, MASSIVE MIMO, BEAMFORMING AND EDGE COMPUTING, IOT, ENCRYPTION, MULTI-LEVEL AUTHENTICATION AND TRAFFIC MONITORING.

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1. ТЕЛЕКОМУНІКАЦІЙНА ІНФРАСТРУКТУРА РОЗУМНОГО МІСТА 11
1.1. Основні компоненти інфраструктури Розумного Міста 11
1.2. Телекомунікаційна архітектура для побудови Розумного Міста 19
РОЗДІЛ 2. МОБІЛЬНІ МЕРЕЖІ П'ЯТОГО ПОКОЛІННЯ В ІНФРАСТРУКТУРІ РОЗУМНОГО МІСТА 31
2.1. Архітектурні особливості мобільних мереж 5G 31
2.2. Можливості та переваги використання 5G в Розумному Місті 43
РОЗДІЛ 3. МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІНФРАСТРУКТУРІ РОЗУМНОГО МІСТА З ВИКОРИСТАННЯМ 5G 51
3.1. Аналіз загроз та вразливостей в інфраструктурі Розумного Міста на основі 5G 51
3.2. Методи забезпечення кібербезпеки на основі мобільних мереж п'ятого покоління 61
ВИСНОВКИ 71
ПЕРЕЛІК ПОСИЛАНЬ 73
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 77

ВСТУП

Розвиток урбанізації та зростання чисельності населення у містах створюють нові виклики для забезпечення ефективного управління міською інфраструктурою, раціонального використання ресурсів та підвищення якості життя громадян. У відповідь на ці виклики концепція розумного міста (Smart City) набуває все більшої актуальності, оскільки вона передбачає використання сучасних інформаційно-комунікаційних технологій для автоматизації міських процесів, підвищення рівня безпеки та стійкості міського середовища.

Розумне місто базується на інтеграції інноваційних технологій, зокрема Інтернету речей (IoT), мобільних мереж п'ятого покоління (5G), великих даних (Big Data), штучного інтелекту (AI) та хмарних обчислень, що дозволяють здійснювати оперативний моніторинг і управління ключовими аспектами міської інфраструктури. Застосування таких технологій сприяє оптимізації транспортних потоків, підвищенню енергоефективності, поліпшенню екологічного стану та розвитку систем «електронного уряду» для надання громадських послуг у режимі реального часу.

Актуальність розумних міст також зумовлена глобальними тенденціями щодо стійкого розвитку та цифровізації суспільства. Сучасні розумні міста є складними соціально-технічними системами, які інтегрують передові цифрові технології для підвищення якості життя мешканців, оптимізації використання ресурсів та забезпечення сталого розвитку. У цьому контексті мобільні мережі п'ятого покоління (5G) відіграють ключову роль, забезпечуючи високошвидкісне з'єднання, низькі затримки та можливість підключення великої кількості пристроїв. Проте, з розширенням цифрової інфраструктури розумних міст, зростає й кількість потенційних кіберзагроз, які можуть мати критичні наслідки для функціонування міських служб та безпеки громадян.

Забезпечення кібербезпеки в інфраструктурі розумного міста з використанням технологій 5G потребує застосування комплексного підходу, що включає використання сучасних методів захисту інформації, таких як

криптографія, сегментація мережі, моніторинг загроз у режимі реального часу та впровадження механізмів штучного інтелекту для виявлення аномалій.

Незважаючи на значні переваги, такі як підвищена пропускна здатність та можливості масштабування, використання 5G у розумних містах створює нові виклики в галузі кібербезпеки, зокрема пов'язані із захистом приватних даних, попередженням кібератак на критичну інфраструктуру та забезпеченням безперервності надання послуг. Тому дослідження та впровадження ефективних методів кіберзахисту є важливим напрямком для забезпечення надійної роботи систем розумного міста та захисту інтересів його мешканців.

Мета роботи – дослідження методів забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління.

Об'єкт дослідження – процес взаємодії Розумного Міста і мереж п'ятого покоління.

Предмет дослідження – методи забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління.

РОЗДІЛ 1. ТЕЛЕКОМУНІКАЦІЙНА ІНФРАСТРУКТУРА РОЗУМНОГО МІСТА

1.1. Основні компоненти інфраструктури Розумного Міста

Інтеграція керування трафіком у реальному часі є проблемою інтелектуальних транспортних систем, ключових для еволюції розумних міст. Розумні міста використовують такі передові технології, як пристрої Інтернету речей (IoT) і аналітика великих даних, щоб ефективно контролювати та керувати транспортними потоками, зменшуючи затори та мінімізуючи затримки в дорозі [1]. Такий динамічний підхід до управління трафіком сприяє оптимальному прокладанню маршрутів, забезпечуючи повне використання потенціалу міських доріг [2]. Обробляючи дані в режимі реального часу, ці системи можуть динамічно коригувати дорожні сигнали та надавати водіям актуальну інформацію про дорожній рух. Це не тільки покращує враження від поїздок, але й сприяє зменшенню споживання палива та викидів, узгоджуючи з цілями сталого розвитку, притаманними дизайну розумних міст. Крім того, інтеграція інтелектуальних рішень для паркування додатково доповнює управління дорожнім рухом, спрямовуючи водіїв до доступних місць для паркування, таким чином скорочуючи час, витрачений на пошук місця для паркування, і покращуючи загальну міську мобільність.

Розвиток автономних транспортних засобів є значним кроком вперед у транспортній складовій інфраструктури розумного міста. Ці транспортні засоби покладаються на складну мережу датчиків, алгоритми машинного навчання та обробку даних у реальному часі для безпечної навігації в складних міських середовищах [3]. Автономні транспортні засоби обіцяють революцію в міській мобільності, пропонуючи безпечніші, ефективніші та екологічно чисті способи пересування. Вони усувають фактор людської помилки, який є основною причиною аварій, тим самим підвищуючи безпеку дорожнього руху. Крім того, автономні транспортні засоби можуть працювати безперервно без втоми,

оптимізуючи транспортний потік і зменшуючи затори в години пік. Цей прогрес у транспортних технологіях є не просто футуристичною концепцією, а відчутним кроком до досягнення повної інтеграції різних компонентів розумного міста, що в кінцевому підсумку покращує якість міського життя [4].

Таблиця 1.1.

Основні компоненти інфраструктури Розумного Міста

	Компонент	Опис
1	Інтелектуальне управління транспортом	Керування трафіком у реальному часі, зменшення
2	Автономні транспортні засоби	Використання датчиків і алгоритмів для автономного водіння
3	Інтелектуальні рішення для громадського транспорту	Відстеження транспорту, інтелектуальні квиткові
4	Стійке управління енергією	Перехід на відновлювані джерела енергії
5	Розумні мережі та розподіл енергії	Моніторинг та балансування енергоспоживання
6	Енергоефективність у громадській інфраструктурі	Зниження витрат через світлодіодне освітлення та HVAC системи
7	Передові комунікаційні мережі (5G)	Забезпечення зв'язку 3 низькою затримкою
8	Інтернет речей (IoT)	Збір та аналіз даних від сенсорних пристроїв
9	Кібербезпека	Захист інфраструктури від кіберзагроз
10	Розумне управління водними	Моніторинг та контроль розподілу води
11	Інтелектуальне управління відходами	Автоматизовані системи збору та сортування відходів
12	Містопланування та розвиток	Застосування ГІС для зонування та планування

	Компонент	Опис
13	Системи громадської безпеки	Системи відеоспостереження та реагування на надзвичайні
14	Електронне врядування та послуги для громадян	Цифрові сервіси для громадян та прозорість управління
15	Інфраструктура охорони здоров'я	Телемедицина, віддалений моніторинг здоров'я

Впровадження інтелектуальних рішень для громадського транспорту є ще одним важливим аспектом розвитку інфраструктури розумного міста. Ці рішення охоплюють відстеження автобусів і поїздів у режимі реального часу, інтелектуальні системи продажу квитків і протоколи прогнозованого технічного обслуговування [5]. Використовуючи технологію GPS і сенсорні мережі, системи громадського транспорту можуть пропонувати оновлення в режимі реального часу пасажирам, підвищуючи надійність і зручність громадського транспорту. Інтелектуальні системи продажу квитків, які дозволяють здійснювати безготівкові та безконтактні платежі, не тільки спрощують процес посадки, але й надають цінні дані для оптимізації графіків обслуговування та маршрутів. Крім того, прогнозне технічне обслуговування на основі аналітики даних гарантує, що транспортні засоби громадського транспорту залишатимуться у відмінному стані, мінімізуючи збої в роботі. Разом ці інтелектуальні рішення сприяють створенню більш стійкої та ефективної системи громадського транспорту, роблячи її життєздатною альтернативою використанню приватного транспорту та сприяючи більш стійкому міському середовищу.

Стійке управління енергією

Включення відновлюваних джерел енергії є фундаментальним аспектом сталого управління енергією в рамках інфраструктури Smart City. Перехід до використання відновлюваної енергії зумовлений необхідністю скорочення викидів вуглецю та сприяння екологічній стійкості. Міста все більше інвестують у сонячні батареї, вітрові турбіни та інші відновлювані технології для використання чистої

енергії. Цей зсув не тільки зменшує залежність від викопного палива, але й підвищує енергетичну безпеку шляхом диверсифікації джерел енергії. Крім того, системи відновлюваної енергетики часто краще адаптуються до міського середовища, дозволяючи локалізоване виробництво енергії, що може значно зменшити втрати при передачі. Впровадження рішень у сфері відновлюваної енергетики є наріжним каменем у розвитку розумних міст, що забезпечує більш чисте та стійке міське середовище [6].

Розумні мережі та розподіл енергії відіграють вирішальну роль в ефективному управлінні енергетичними ресурсами в розумному місті. Інтелектуальна мережа — це розширена електрична мережа, яка використовує цифрові технології для моніторингу та керування транспортуванням електроенергії з усіх джерел генерації, щоб задовольнити різні потреби кінцевих споживачів в електроенергії. Ця система дозволяє збирати й аналізувати дані в режимі реального часу, забезпечуючи краще реагування на попит і балансування навантаження. Завдяки інтеграції інтелектуальних лічильників і датчиків, інтелектуальні мережі сприяють двосторонньому потоку електроенергії та інформації, підвищуючи надійність і зменшуючи витрати енергії. Розгортання інтелектуальних мереж має важливе значення для оптимізації розподілу енергії, підвищення стійкості мережі та підтримки інтеграції відновлюваних джерел енергії в міський енергетичний баланс [7].

Енергоефективність у громадській інфраструктурі є ще одним важливим компонентом сталого управління енергією в розумних містах. Громадські будівлі, вуличне освітлення та транспортні системи є значними споживачами енергії, і оптимізація їх використання енергії може призвести до суттєвої економії. Впровадження енергоефективних технологій, таких як світлодіодне освітлення, інтелектуальні системи опалення, вентиляції, вентиляції та кондиціонування повітря та програмне забезпечення для управління енергією, може значно зменшити споживання енергії в цих інфраструктурах. Крім того, модернізація існуючих будівель енергозберігаючими технологіями може ще більше підвищити ефективність і продуктивність. Ці заходи не тільки знижують експлуатаційні

витрати, але й сприяють досягненню екологічних цілей щодо скорочення викидів парникових газів. Зосереджуючись на енергоефективності, розумні міста можуть досягти більш стійкого та економічно ефективного міського середовища [8].

Advanced Communication Networks

Розгортання технології 5G є ключовим прогресом у розвитку передових комунікаційних мереж у розумних містах. Ця мобільна мережа наступного покоління — це не просто оновлення, а трансформаційний стрибок, який забезпечує надшвидке підключення, забезпечуючи безперебійний зв'язок і передачу даних між різними міськими інфраструктурами. Інтеграція технології 5G дозволяє використовувати існуючі інфраструктури 4G, що значно полегшує процес переходу та скорочує витрати, пов'язані з повною реконструкцією існуючих мереж [9]. Характеристики високої швидкості та низької затримки 5G роблять його особливо придатним для підтримки великих потреб у даних у додатках розумного міста, таких як керування трафіком у реальному часі та системи реагування на надзвичайні ситуації. Отже, широке впровадження технології 5G має фундаментальне значення для реалізації повного потенціалу розумних міст шляхом підтримки широкого спектру інноваційних послуг і програм.

Підключення до Інтернету речей (IoT) є ще одним важливим аспектом передових комунікаційних мереж у розумних містах. IoT означає мережу взаємопов'язаних фізичних пристроїв із вбудованими датчиками та програмним забезпеченням, які спілкуються та обмінюються даними через Інтернет [10]. Ця мережева концепція є невід'ємною частиною розумних міст, оскільки дозволяє створювати інтелектуальні системи, які покращують міське життя. Використовуючи IoT, міста можуть покращувати різноманітні послуги, такі як управління відходами, водопостачання та громадський транспорт, збираючи та аналізуючи дані в режимі реального часу. Архітектура IoT охоплює численні компоненти, включаючи речі (пристрої), локальні мережі та протоколи зв'язку, які працюють разом, щоб забезпечити ефективні рішення міських проблем [11]. Оскільки IoT продовжує розширюватися, його роль у розумних містах ставатиме все більш важливою, пропонуючи інноваційні рішення для сталого розвитку міст.

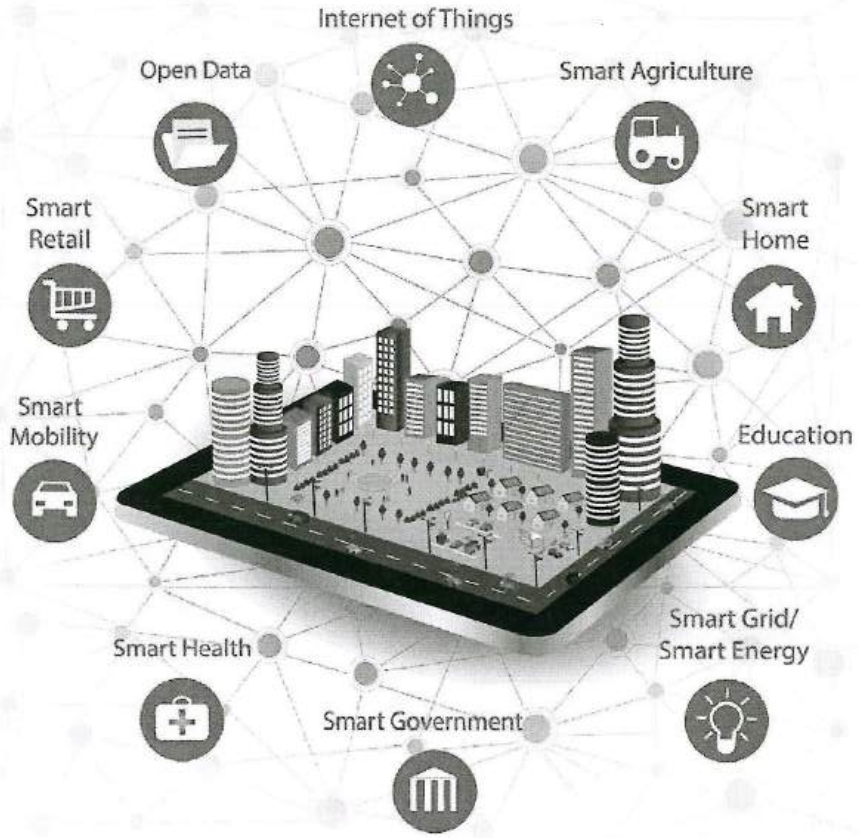


Рис. 1.1. Технології Розумного Міста

Оскільки розумні міста продовжують рости та значною мірою покладаються на взаємопов'язані технології, впровадження надійних заходів кібербезпеки для захисту даних стає все більш вирішальним. Критична інфраструктура міста, включаючи його мережі передачі даних, сприйнятлива до кіберзагроз, що вимагає комплексних стратегій для захисту конфіденційної інформації від потенційних зломів [12]. Кібербезпека в розумних містах передбачає розгортання передових методів шифрування, регулярні перевірки безпеки та системи моніторингу в реальному часі для виявлення та запобігання несанкціонованому доступу. Важливо розуміти основні кіберзагрози для пристроїв IoT, оскільки ці пристрої утворюють основу інфраструктури розумного міста [13]. Забезпечуючи надійні заходи захисту даних, міста можуть підтримувати цілісність і надійність своїх інтелектуальних систем, зміцнюючи довіру між жителями та зацікавленими сторонами, одночасно сприяючи безпечному та стійкому міському середовищу.

Smart Water Management

У сфері інфраструктури розумного міста моніторинг якості води та її розподілу в реальному часі відіграють ключову роль у забезпеченні ефективного та сталого управління водними ресурсами. Передові технології, такі як бездротові сенсорні мережі (WSN), забезпечують надійну платформу для збору даних про параметри якості води, такі як pH, температура та каламутність, а також відстеження розподілу води по міській мережі [2]. Цей збір даних у реальному часі дозволяє муніципалітетам оперативно вирішувати будь-які проблеми, пов'язані із забрудненням води, витоками або неефективністю розподілу. Інтегруючи ці передові системи моніторингу, міста можуть покращити розподіл ресурсів, зменшити марнотратство води та підвищити загальну надійність мережі водопостачання. Оскільки міста продовжують рости та стикаються зі зростаючим попитом на водні ресурси, впровадження таких інтелектуальних технологій стає необхідним для підтримки екологічної стійкості та здоров'я населення.

Технології виявлення витоків і зменшення відходів є життєво важливими компонентами інтелектуальних систем управління водою, спрямованих на оптимізацію використання води та мінімізацію втрат. Інновації в сенсорних технологіях і аналітиці даних дозволили виявляти витоки в реальному часі, дозволяючи швидко діяти, щоб запобігти втраті води. Наприклад, акустичні датчики можуть ідентифікувати звук води, що витікає з труб, тоді як датчики тиску виявляють аномалії потоку води, які можуть вказувати на витік. Ці системи не тільки допомагають економити воду, але й зменшують витрати, пов'язані з втратою води та ремонтом інфраструктури. Крім того, використовуючи алгоритми машинного навчання, ці технології можуть передбачати потенційні витоки до того, як вони відбудуться, тим самим покращуючи стратегії профілактичного обслуговування міських систем водопостачання. По суті, впровадження цих передових технологій виявлення витоків є вирішальним кроком до досягнення сталого управління водними ресурсами в розумних містах.

Сталі процеси очищення та переробки води є фундаментальними для парадигми розумного управління водними ресурсами, сприяючи збереженню навколишнього середовища та ефективності використання ресурсів. Інтеграція

передових технологій, таких як мембранна фільтрація, процеси біологічного очищення та передові методи окислення, дозволяє ефективно очищати стічні води. Ці технології гарантують, що очищена вода відповідає необхідним стандартам безпеки та якості, що робить її придатною для повторного використання в різних непитних цілях, таких як зрошення та промислові процеси. Переробка очищених стічних вод не тільки зберігає ресурси прісної води, але й зменшує вплив скидання стічних вод на навколишнє середовище. Застосовуючи стійкі практики очищення та переробки води, розумні міста можуть значно пом'якшити проблеми дефіциту води та зробити внесок у більш стійку міську екосистему. У міру того, як ці практики набувають більшого поширення, вони відіграватимуть дедалі важливішу роль у розвитку сталого міського середовища.

Розумне управління відходами

Інтеграція автоматизованих систем збору відходів є наріжним каменем у розвитку інфраструктури розумного міста. Ці системи, такі як пневматична конвеєрна система відходів, використовують підземні трубопроводи для ефективного та непомітного транспортування відходів із житлових і комерційних районів до центральних пунктів збору [14]. Цей метод не тільки мінімізує візуальний і нюховий вплив збору відходів на міське середовище, але й значно скорочує трудові та транспортні витрати, пов'язані з традиційними методами поводження з відходами. Автоматизовані системи спрощують весь процес, роблячи утилізацію відходів ефективнішою та менш нав'язливою. Крім того, скорочення руху транспортних засобів для збирання відходів сприяє зменшенню викидів парникових газів, що відповідає ширшим цілям сталого розвитку.

Удосконалення технологій сортування та переробки сміття мають вирішальне значення для ефективного поводження з міськими відходами в розумних містах. Ці технології використовують машинне навчання та автоматизацію для точного сортування матеріалів, що підлягають переробці, із звичайних потоків відходів [15]. Підвищуючи точність процесів сортування, інтелектуальні системи управління відходами підвищують ефективність переробки та зменшують кількість відходів, які відправляються на звалища. Ключові

технологічні інновації включають машини для сортування на основі датчиків, які можуть ідентифікувати та розділяти матеріали на основі їх складу та кольору. Це не тільки оптимізує відновлення ресурсів, але й підтримує циклічну економіку, забезпечуючи постійне повторне введення цінних матеріалів у виробничий цикл. Ці технології є ключовими для міст, які прагнуть мінімізувати свій вплив на навколишнє середовище.

Стратегії управління відходами на основі даних стають все більш важливими, оскільки міста прагнуть оптимізувати свої процеси управління відходами. Використовуючи аналітику даних та інформаційні технології, розумні міста можуть приймати обґрунтовані рішення щодо збору та обробки відходів [14]. Ці стратегії передбачають збір даних у режимі реального часу про моделі утворення відходів, які можна використовувати для прогнозування попиту на послуги зі збору відходів і оптимізації маршрутів збору. Крім того, аналітика даних дозволяє містам визначати райони з високим утворенням відходів і відповідним чином пристосовувати заходи з утилізації відходів. Такий підхід не тільки підвищує ефективність операцій з утилізації відходів, але й сприяє прозорості та підзвітності, надаючи зацікавленим сторонам доступ до повних даних щодо утилізації відходів. Роблячи це, міста можуть сприяти залученню громади та заохочувати практику сталого поводження з відходами серед мешканців.

1.2. Телекомунікаційна архітектура для побудови Розумного Міста

Вимоги до телекомунікаційної інфраструктури

Основні компоненти телекомунікаційної інфраструктури в «смарт-місті» включають різноманітні елементи, які забезпечують ефективну передачу та обробку даних. Важливими аспектами є мережі передачі даних, системи зберігання інформації та різноманітні платформи для управління даними. Наприклад, корпоративні мережі створюють всю комунікаційну інфраструктуру, що забезпечує взаємодію користувачів із спеціальними типами термінальних

пристроїв і кабельними системами [4]. Ці компоненти є основою для створення інтегрованої надійної мережі, яка підтримує функціонування всіх елементів "розумного міста". Без них неможливо забезпечити безперебійний обмін інформацією, необхідний для реалізації функцій смарт-міста, таких як розумні системи охорони здоров'я та управління транспортом.

Таблиця 1.2.

Вимоги до телекомунікаційної інфраструктури

Категорія	Опис
Продуктивність	Висока пропускна здатність, низька затримка, підтримка великої кількості підключень
Надійність	Безперервність роботи, резервування ресурсів, відновлення після збоїв
Безпека	Шифрування, аутентифікація, захист від несанкціонованого доступу
Масштабованість	Можливість розширення мережі відповідно до зростаючих потреб
Сумісність	Підтримка різних стандартів та протоколів для інтеграції
Енергоефективність	Оптимальне використання енергоресурсів для зниження витрат
Конфіденційність	Захист персональних даних, відповідність законодавчим нормам
Гнучкість	Адаптація до нових технологій та змін у середовищі
Доступність	Доступ до послуг у будь-який час та з будь-якого місця

Високошвидкісний Інтернет та мережі передачі даних виконують критичну роль у телекомунікаційних структурах смарт-міста. Вони забезпечують швидке з'єднання та обмін даними між безкоштовними пристроями та системами, що є основою для реалізації смарт-рішень. Наприклад, структура 5G надає послуги з високошвидкісною передачею даних, що дозволяє ефективно контролювати

передачу даних мережею, використовуючи програмно-визначені мережі (SDN) [5]. Це дозволяє не тільки покращити якість обслуговування, але й забезпечити більш надійну та безперебійну роботу всіх систем смарт-міста. Високошвидкісні мережі також сприяють розвитку інноваційних сервісів, таких як автоматизоване управління трафіком та екологічний моніторинг.

Інтеграція пристроїв і датчиків IoT є ще одним аспектом телекомунікаційної інфраструктури смарт-міста. Ці пристрої дозволяють збирати, аналізувати та використовувати величезні обсяги даних для прийняття обґрунтованих рішень у реальному часі. Як показано в наукових дослідженнях, платформи Інтернету говорять про важливу роль у смарт-містах, пропонуючи різні підходи до впровадження смарт-систем [6]. Це включає в себе інтеграцію сенсорних даних та інформації зі спеціалізованих IoT-пристроїв, що дозволяє підвищити ефективність управління ресурсами міста та забезпечити кращий рівень комфорту для його мешканців. Завдяки цьому IoT-пристрої залишаються невід'ємною частиною сучасної телекомунікаційної архітектури смарт-міст.

Мережеві технології для розумних міст

Бездротові технології, такі як 5G і Wi-Fi 6, є наріжними каменями розумних міст, забезпечуючи високошвидкісний доступ до мережі та підтримуючи перервний потік даних серед різноманітних пристроїв та систем. Крім того, технологія 5G пропонує лише низьку затримку та високу пропускну здатність, що робить її ідеальною для підтримки великої кількості пристроїв IoT, які є максимальною для роботи розумного міста [7]. Wi-Fi 6, з іншого боку, забезпечує підвищену ефективність в умовах високої щільності підключення, що дозволяє забезпечити стабільне підключення навіть у найбільш населених районах [8]. Ці бездротові технології допомагають створити мережеву інфраструктуру, яка може адаптуватися до зростаючих потреб сучасних міських середовищ.

Волоконно-оптичні мережі також виконують важливу роль у розвитку телекомунікаційних систем розумних міст завдяки своїм численним перевагам. Одна з головних переваг оптоволоконних мереж полягає в їх здатності забезпечити високовисоку швидкість передачі даних на високу швидкість без втрати сигналу

[9]. Це робить їх ідеальними для використання в критично важливих системах, де надійність і швидкість є пріоритетними. Крім того, оптичні мережі вимагають менше енергії для обробки великого обсягу даних, що сприяє створенню більш екологічно стійкої інфраструктури. Ці мережі можуть бути основою для ефективного управління даними, необхідними для інтеграції різних підсистем розумного міста.

Системи супутникового зв'язку забезпечують додатковий рівень покриття та гнучкості, які є критичними для інфраструктури розумного міста, особливо в географічно віддалених або важкодоступних районах. Супутниковий зв'язок дозволяє забезпечити підключення там, де традиційні глобальні мережі не можуть бути розгорнуті через фізичні обмеження або економічну недоцільність [10]. Це робить супутникові системи незамінними для забезпечення безперервності зв'язку в умовах катастроф або інших надзвичайних ситуацій. Крім того, вони можуть використовуватися для підтримки різних програм, від моніторингу навколишнього середовища до надання послуг екстреної допомоги, що робить їх компонентом стратегії розумного міста.

Управління та безпека даних

Ефективне управління величезними обсягами даних є наріжним каменем телекомунікаційної архітектури розумного міста. Оскільки міста стають більш взаємопов'язаними, вони генерують і накопичують значні обсяги даних із різних джерел, таких як датчики, пристрої Інтернету речей і системи спостереження. Щоб ефективно керувати цими даними, розумні міста використовують передові стратегії керування даними, які включають хмарні рішення для зберігання даних, озера даних і аналітичні платформи в реальному часі. Ці технології дозволяють містам швидко обробляти та аналізувати дані, дозволяючи приймати більш обґрунтовані рішення та покращувати міські послуги [11]. Наприклад, дані про дорожній рух у реальному часі можна використовувати для оптимізації транспортного потоку, зменшення заторів і вдосконалення систем громадського транспорту. Використовуючи ці стратегії, розумні міста можуть забезпечити не

тільки ефективне зберігання величезної кількості згенерованих даних, але й використання максимально повного потенціалу.

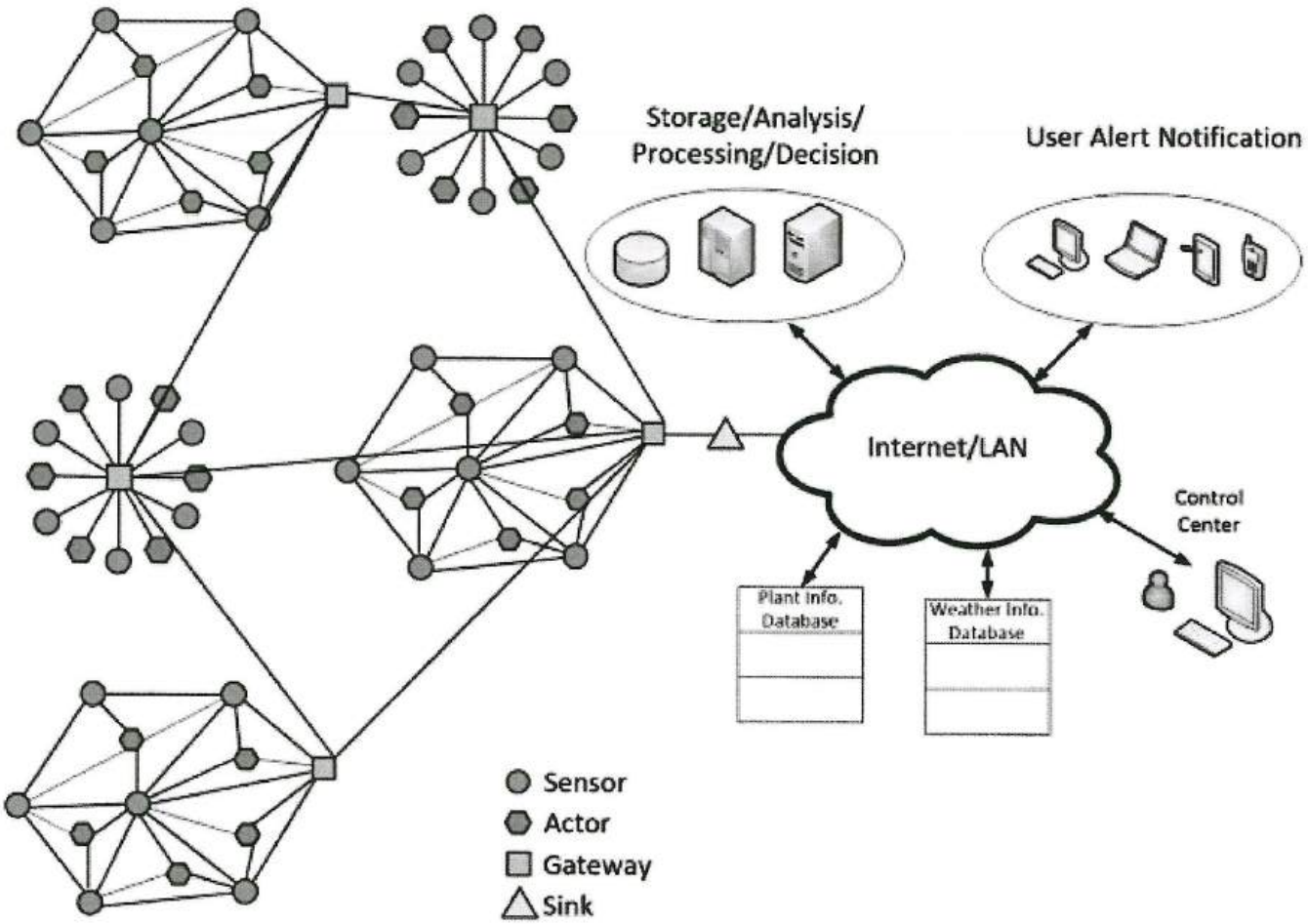


Рис. 1.2. Телекомунікаційна архітектура для побудови Розумного Міста

Важливість конфіденційності та безпеки даних неможливо переоцінити в контексті розумних міст. Оскільки міста все більше покладаються на цифрові платформи та пристрої IoT для управління міською інфраструктурою, ризик витоку даних і несанкціонованого доступу також зростає. Забезпечення конфіденційності конфіденційної інформації, такої як персональні дані, зібрані від громадян, має вирішальне значення для підтримки громадської довіри та дотримання нормативних актів [11]. У розумних містах застосовуються надійні заходи кібербезпеки, включаючи шифрування, контроль доступу та безпечні протоколи зв'язку, щоб захистити конфіденційність даних. Крім того, впровадження суворої

політики управління даними гарантує, що дані обробляються відповідально та етично. У результаті міста можуть захистити свої цифрові екосистеми, водночас створюючи середовище, у якому можуть процвітати інновації та технологічний прогрес.

Забезпечення цілісності та надійності даних має важливе значення для успішної роботи інфраструктури розумного міста. Цілісність даних означає точність і узгодженість даних протягом їх життєвого циклу, що має вирішальне значення для прийняття надійних рішень на основі цих даних. Щоб досягти цього, розумні міста впроваджують різні методи, такі як перевірка даних, виявлення помилок і системи резервування, щоб запобігти пошкодженню та втраті даних. Ці методи допомагають підтримувати достовірність даних, дозволяючи міським планувальникам і адміністраторам покладатися на точну інформацію для стратегічного планування та оперативної ефективності [12]. Крім того, регулярні аудити та моніторинг систем даних додатково підвищують надійність даних, забезпечуючи міцну основу для постійного вдосконалення міських послуг і добробуту громадян.

Протоколи зв'язку Smart City

У сфері розумних міст комунікаційні протоколи служать основою для безперебійної взаємодії між різними пристроями та системами. Ці протоколи забезпечують ефективну та надійну передачу даних через мережу взаємопов'язаних пристроїв. Огляд існуючих стандартів розумного міста має вирішальне значення для зацікавлених сторін, залучених до цих проектів, оскільки це допомагає їм зрозуміти технічний і нормативний ландшафт, яким вони повинні орієнтуватися [13]. Найбільш відомі стандарти та протоколи, такі як MQTT, XMPP та інші, відіграють ключову роль у впровадженні рішень IoT у розумних містах, дозволяючи пристроям ефективно та безпечно спілкуватися [7]. Ці протоколи мають важливе значення для керування величезним потоком даних, створених додатками розумних міст, гарантуючи, що інформація є доступною та дієвою.

Сумісність між пристроями є фундаментальним аспектом розвитку розумного міста. Без взаємодії різноманітні датчики, лічильники та комунікаційні

пристрої, що використовуються в розумних містах, не можуть функціонувати злагоджено [14]. Ця сумісність гарантує, що дані, зібрані з різних джерел, можуть бути інтегровані та максимально використані. Створення програм Smart City значною мірою залежить від здатності контролювати зв'язок між пристроями, наприклад, у бездротових сенсорних мережах (WSN) [11]. Встановивши загальну комунікаційну структуру, розумні міста можуть оптимізувати свою діяльність, покращити розподіл ресурсів і надавати кращі послуги своїм громадянам. Ця сумісність також підтримує інновації, дозволяючи бездоганно інтегрувати нові технології в існуючу інфраструктуру.

Стандартизація протоколів зв'язку в розумних містах викликає кілька проблем. Однією з важливих проблем є відсутність уніфікованості стандартів у різних регіонах і виробниках, що може призвести до фрагментації та неефективності [14]. Більше того, швидкі темпи технологічного прогресу означають, що протоколи необхідно постійно оновлювати та вдосконалювати для адаптації до нових пристроїв і програм. Це динамічне середовище ускладнює встановлення стабільного набору стандартів, які можна прийняти в усьому світі [6]. Незважаючи на ці проблеми, зусилля щодо гармонізації протоколів тривають з метою створення більш згуртованої та ефективної екосистеми розумного міста. Вирішення цих проблем стандартизації має вирішальне значення для забезпечення довгострокового успіху та стійкості розумних міст у всьому світі.

Роль хмарних обчислень

Інтеграція хмарних обчислень в інфраструктуру розумних міст пропонує численні переваги, які значно підвищують ефективність і функціональність міських територій. Однією з основних переваг є масштабованість хмарних ресурсів, яка дозволяє розумним містам обробляти величезні обсяги даних, створених різними підключеними пристроями, не відчуваючи вузьких місць продуктивності [15]. Ця масштабованість гарантує, що в міру зростання міста та додавання нових пристроїв інфраструктура зможе бездоганно задовольняти зростаючий попит.

Таблиця 1.3.

Телекомунікаційна архітектура для побудови Розумного Міста

	Компонент	Призначення	Переваги
1	Мережі передачі даних	Забезпечення ефективної передачі даних у смарт-місті	Швидке та надійне підключення між системами
2	Системи зберігання інформації	Обробка та зберігання великих обсягів міських даних	Безпека та масштабованість
3	Корпоративні мережі	Інтеграція користувачів і термінальних пристроїв	Гнучкість інтеграції з іншими системами
4	Мережеві технології (5G, Wi-Fi 6)	Підтримка безперебійного зв'язку 3 низькою	Висока пропускна здатність і низька затримка
5	Волоконно-оптичні мережі	Високошвидкісний зв'язок для критичних додатків	Надійність та енергоефективність
6	Супутниковий зв'язок	Забезпечення зв’язку у віддалених районах	Глобальне покриття та резервування зв'язку
7	IoT-пристрої та сенсори	Збір даних у реальному часі для міських систем	Оперативний моніторинг міської інфраструктури
8	Хмарні обчислення	Обробка даних на вимогу та масштабування	Гнучкість, економія ресурсів
9	Системи безпеки та управління доступом	Захист телекомунікацій ної інфраструктури	Підвищення рівня кібербезпеки

Крім того, хмарні обчислення забезпечують економічно ефективні рішення, зменшуючи потребу в значних інвестиціях у фізичне обладнання, дозволяючи містам більш ефективно розподіляти ресурси та зосереджуватися на покращенні послуг для жителів [11]. Гнучкість хмарної інфраструктури підтримує широкий спектр застосувань, від інтелектуальних систем освітлення до розширеного управління транспортом, які разом сприяють досягненню головної мети покращення якості життя мешканців [16].

Різні типи хмарних сервісів відіграють вирішальну роль у функціонуванні та розвитку розумних міст, кожен із яких пропонує унікальні можливості, які задовольняють різноманітні міські потреби. Програмне забезпечення як послуга (SaaS) дозволяє містам швидко розгортати програми, полегшуючи керування такими послугами, як контроль дорожнього руху та громадська безпека. Платформа як послуга (PaaS) надає розробникам надійне середовище для створення та розгортання спеціальних програм, які відповідають конкретним потребам міста [17]. Інфраструктура як послуга (IaaS) надає необхідні обчислювальні ресурси, такі як віртуальні машини та сховище, які підтримують магістраль операцій розумного міста. Ці хмарні сервіси гарантують, що міста можуть ефективно розгортати та масштабувати програми, надаючи необхідну технологічну підтримку для підтримки безперервності роботи та покращення міського середовища [2].

Безпека та конфіденційність є першорядними проблемами у сфері хмарних обчислень для розумних міст, оскільки величезна кількість даних, що обробляються та зберігаються, включає конфіденційну інформацію про мешканців і міські операції. Реалізація надійних заходів безпеки, таких як шифрування та контроль доступу, має важливе значення для захисту даних від несанкціонованого доступу та порушень [7]. Крім того, забезпечення дотримання відповідних норм і стандартів допомагає підтримувати довіру між мешканцями та зацікавленими сторонами, створюючи безпечне середовище для обміну та обробки даних. Міркування щодо конфіденційності є не менш важливими, оскільки вони вимагають прозорих практик управління даними, які поважають права людей і

водночас дозволяють інноваційне використання даних для покращення міських послуг. Вирішуючи ці проблеми, розумні міста можуть використовувати хмарні обчислення не тільки для підвищення ефективності роботи, але й для захисту конфіденційності та безпеки своїх мешканців [18].

Впровадження служб Smart City

Архітектура телекомунікацій відіграє ключову роль у розгортанні послуг Smart City, забезпечуючи надійну структуру для різноманітних програм і послуг. Інтеграція хмарних технологій у традиційний телекомунікаційний стек дозволяє розумним містам пропонувати складні послуги, такі як віртуальні машини, які можна надавати як послугу для підтримки різноманітних міських програм [19]. Ця можливість дозволяє містам ефективно керувати ресурсами та надавати такі послуги, як моніторинг дорожнього руху в реальному часі, управління енергією та покращення громадської безпеки. Крім того, розгортання волоконно-оптичної мережі формує основу цих телекомунікаційних мереж, забезпечуючи високошвидкісне та надійне з'єднання по всьому місту [20]. Ця інфраструктура підтримує безперебійну роботу сервісів розумного міста, сприяючи ефективній передачі даних і покращуючи якість життя мешканців.

Телекомунікаційна архітектура суттєво впливає на транспортний і комунальний сектори в розумних містах, забезпечуючи передові рішення мобільності та ефективне управління ресурсами. Наприклад, розумні транспортні системи використовують телекомунікаційні мережі для оптимізації потоку трафіку та зменшення заторів за допомогою аналізу даних у реальному часі та адаптивних систем керування трафіком [14]. Ці системи використовують відеоспостереження та сенсорні мережі для моніторингу умов дорожнього руху та відповідного коригування сигналів, забезпечуючи більш плавні поїздки на роботу та роботу та покращуючи безпеку на дорогах [21]. Так само в комунальному секторі телекомунікації сприяють інтеграції інтелектуальних мереж, які дозволяють динамічно розподіляти енергію та контролювати споживання. Ця можливість зменшує витрати енергії та покращує надійність обслуговування. Стратегічне розміщення датчиків і пристроїв Інтернету речей по всьому місту ще більше

покращує ці сектори, надаючи безцінні дані особам, які приймають рішення, що веде до більш обґрунтованого міського планування та ефективного розподілу ресурсів.

У сфері громадської безпеки та реагування на надзвичайні ситуації телекомунікаційна архітектура відіграє важливу роль у розширенні можливостей розумних міст. Інтеграція передових інформаційно-комунікаційних технологій дозволяє швидко реагувати на надзвичайні ситуації та покращує координацію між органами громадської безпеки [22]. Наприклад, розумні міста використовують складні системи спостереження та комунікаційні мережі для швидкого виявлення і реагування на інциденти, тим самим знижуючи рівень злочинності та підвищуючи довіру населення до заходів безпеки [23]. Крім того, завдяки розгортанню пристроїв і датчиків Інтернету речей міста можуть стежити за станом навколишнього середовища та потенційними небезпеками, забезпечуючи своєчасне оповіщення та профілактичні заходи у разі надзвичайних ситуацій. Цей проактивний підхід не тільки підвищує ефективність систем реагування на надзвичайні ситуації, але й сприяє загальній стійкості міської інфраструктури. У результаті розумні міста краще оснащені для захисту своїх громадян і підтримки громадської безпеки в міському ландшафті, що постійно змінюється.

Проблеми в телекомунікаційній архітектурі

Однією з головних технічних проблем у розгортанні телекомунікаційної інфраструктури для розумних міст є інтеграція різноманітних систем. Інтернет речей (IoT) утворює основу архітектур розумних міст, об'єднуючи численні пристрої та датчики для збору й аналізу даних. Однак для інтеграції цих систем потрібна надійна структура для роботи з різними протоколами та стандартами зв'язку [24]. Наприклад, архітектура fog computing, яка служить проміжним шаром між хмарними та периферійними пристроями, повинна бути ретельно розроблена, щоб забезпечити безперебійний потік даних і обробку [25]. Крім того, швидкі темпи урбанізації загострюють ці технічні проблеми, оскільки інфраструктура має бути масштабованою, щоб відповідати зростаючому населенню та його вимогам [25].

Розподіл фінансових ресурсів і управління фіскальною політикою створюють значні перешкоди для розвитку телекомунікацій у розумних містах. Фінансування має важливе значення не лише для початкового розгортання інфраструктури, але й для її поточного обслуговування та модернізації [26]. Особи, які приймають рішення, повинні зробити стратегічний вибір щодо того, куди розподілити кошти, збалансувавши нагальні потреби з довгостроковою стабільністю. Крім того, фінансові обмеження часто призводять до проблем із визначенням пріоритетів, коли певні проекти можуть отримувати фінансування за рахунок інших, що потенційно може призвести до прогалин у послугах чи інфраструктурі [26]. Ефективне фінансове планування та управління ресурсами мають вирішальне значення для того, щоб телекомунікаційна архітектура розумного міста могла ефективно підтримувати заплановані функції.

Регуляторні та політичні бар'єри також перешкоджають розвитку телекомунікаційної інфраструктури для розумних міст. Динамічний характер технологічного прогресу часто випереджає існуючі правила, створюючи невідповідність між тим, що технологічно можливо, і тим, що дозволено законом [26]. Уряди та регуляторні органи повинні співпрацювати, щоб оновити політику, яка сприятиме інтеграції нових технологій, одночасно захищаючи суспільні інтереси. Політична воля є важливою для стимулювання цих змін, оскільки зацікавлені сторони повинні співпрацювати, щоб подолати бюрократичну інерцію та опір змінам [26]. Крім того, міжнародна співпраця та стандартизація можуть сприяти більш уніфікованому підходу до регуляторних проблем, дозволяючи містам легше застосовувати найкращі практики та інноваційні рішення.

РОЗДІЛ 2. МОБІЛЬНІ МЕРЕЖІ П'ЯТОГО ПОКОЛІННЯ В ІНФРАСТРУКТУРІ РОЗУМНОГО МІСТА

2.1. Архітектурні особливості мобільних мереж 5G

Нарізка мережі (Network Slicing)

Нарізка мережі — це революційна концепція в архітектурі 5G, яка фундаментально змінює структуру та використання мобільних мереж. Цей метод дозволяє кільком логічним мережам співіснувати в одній фізичній мережевій інфраструктурі, кожна з яких адаптована для конкретних програм або послуг [1]. Завдяки цьому він може оптимізувати розподіл ресурсів, підвищити ефективність мережі та забезпечити безперешкодне виконання різноманітних вимог до послуг. Основною метою нарізки мережі є надання індивідуальних мережевих рішень, які задовольняють різноманітні потреби клієнтів, будь то низька затримка для ігрових програм або висока надійність для критично важливих комунікацій. Ця гнучкість є значним відхиленням від попередніх поколінь мереж, які були більш жорсткими та менш адаптованими до різноманітних вимог.

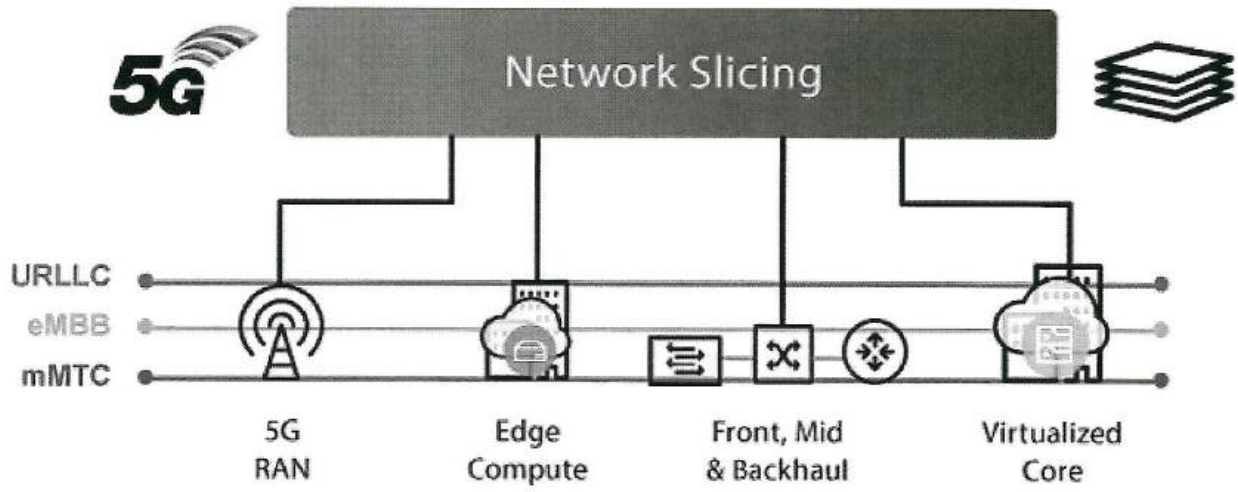


Рис. 2.1. Нарізка мережі (Network Slicing)

Реалізація нарізки мережі в 5G включає складні методи, які забезпечують безперебійну роботу в різних сегментах мережі. Кожен фрагмент налаштований відповідно до певних показників продуктивності та угод про рівень обслуговування, що дозволяє постачальникам послуг пропонувати диференційовані послуги з унікальними характеристиками [1]. Наприклад, один сегмент може надавати пріоритет низькій затримці та високій швидкості для додатків автономного транспорту, тоді як інший зосереджується на масовому підключенні для пристроїв IoT. Це досягається за допомогою вдосконалених систем керування мережею, які динамічно розподіляють ресурси та адаптуються до умов мережі в реальному часі. Використання технологій віртуалізації та програмно-визначених мереж (SDN) є невід'ємною частиною цього процесу, забезпечуючи швидкість і гнучкість, необхідні для керування кількома віртуальними мережами в одній фізичній структурі.

Переваги нарізки мережі в 5G численні, пропонуючи розширені можливості та програми, які раніше були недоступні зі старими мережевими технологіями. Однією з ключових переваг є можливість надавати індивідуальні мережеві рішення, які відповідають конкретним потребам різних галузей, від охорони здоров'я до розваг [2]. Ця настройка покращує продуктивність і покращує взаємодію з користувачем, оскільки кожен фрагмент оптимізовано відповідно до призначення. Крім того, нарізка мережі підтримує швидке розгортання нових служб, оскільки дозволяє швидко й ефективно створювати нові зрізи без необхідності масштабних змін фізичної інфраструктури. Це не тільки зменшує витрати, але й прискорює інновації, дозволяючи постачальникам послуг швидко реагувати на вимоги ринку та технологічний прогрес.

Massive MIMO (Multiple Input Multiple Output)

Технологія MIMO, що розшифровується як Multiple Input Multiple Output, є критично важливим компонентом сучасних систем бездротового зв'язку [3]. Це дозволяє передавати та приймати кілька сигналів даних одночасно по одному радіоканалу, значно підвищуючи пропускну здатність даних і спектральну

ефективність. Це досягається за рахунок використання кількох антен як на стороні передавача, так і на приймачі, створюючи кілька шляхів для передачі даних. Ця концепція використовує просторове рознесення, забезпечуючи більш надійну передачу даних навіть у складних умовах з перешкодами або перешкодами. Технологія MIMO відіграла важливу роль у розвитку бездротового зв'язку, заклавши основу для підвищення вимог до мереж 5G.

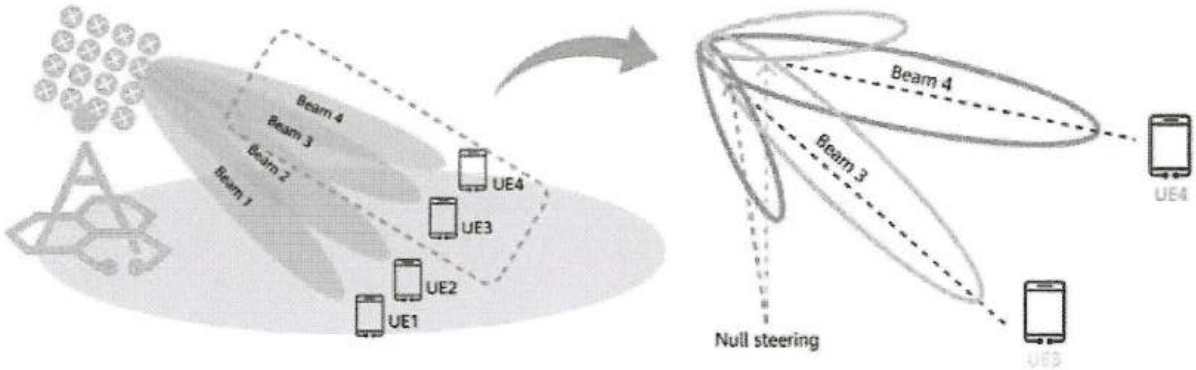


Рис. 2.2. Massive MIMO і Beamforming

Масивний MIMO відіграє ключову роль у збільшенні пропускної здатності мережі систем 5G, що має вирішальне значення для боротьби з очікуваним сплеском трафіку даних [4]. Завдяки розгортанню великої кількості антен на базовій станції масивний MIMO може обслуговувати кількох користувачів одночасно, кожен зі своїм унікальним потоком даних. Ця технологія не тільки підвищує загальну пропускну здатність, але й покращує енергоефективність мережі, фокусуючи енергію передачі безпосередньо на призначеного користувача, тим самим зменшуючи перешкоди. Можливість керувати великою кількістю антен дозволяє точніше формувати промінь, що спрямовує сигнали до конкретних користувачів, підвищуючи як швидкість, так і надійність. Це особливо важливо в густонаселених районах, де попит на мережу високий.

Незважаючи на свої переваги, розгортання масивної технології MIMO представляє кілька проблем, які потребують ретельного розгляду та інноваційних рішень [3]. Однією з основних проблем є складність обробки сигналу, оскільки

робота великої кількості антен вимагає складних алгоритмів для ефективного керування потоками даних і мінімізації перешкод. Крім того, фізичні розміри та вартість розміщення багатьох антен можуть бути непомірно високими, особливо в міських умовах з обмеженим простором. Щоб вирішити ці проблеми, дослідники вивчають передові методи, такі як машинне навчання для оптимізації обробки сигналу та розробки більш компактних конструкцій антен. Крім того, для забезпечення успішного впровадження масової MIMO в мережах 5G необхідно розглянути регуляторні міркування щодо електромагнітного впливу та розподілу спектру.

Beamforming

Формування променя є ключовим методом у мережах 5G, призначеним для підвищення якості сигналу та ефективності передачі даних. Спрямовуючи потужність передачі на конкретних користувачів або пристрої, формування променя мінімізує перешкоди та максимізує використання доступного спектру [5]. Це досягається шляхом регулювання фази та амплітуди сигналів на антенній решітці, створюючи сфокусовані промені, які можуть динамічно адаптуватися до місця розташування користувача. Ця точність забезпечує цільовий зв'язок, що особливо корисно в густонаселеному міському середовищі, де попит на мережу високий. Покращуючи співвідношення сигнал/шум, формування променя не тільки покращує зв'язок, але й підтримує більш високу швидкість передачі даних і більш надійний зв'язок.

Переваги формування променя в мережах 5G численні та трансформаційні. Однією з істотних переваг є збільшена пропускна здатність і покриття, оскільки формування променя дозволяє мережі підтримувати більше користувачів без шкоди для якості. Це має вирішальне значення для задоволення зростаючих вимог програм, що вимагають високої пропускної здатності та низької затримки, таких як віртуальна реальність і автономні транспортні засоби [6]. Крім того, формування променя сприяє енергоефективності, спрямовуючи сигнали саме туди, куди потрібно, зменшуючи втрати енергії. Цей цільовий підхід також підвищує безпеку, оскільки сфокусовані промені ускладнюють перехоплення комунікацій

неавторизованим користувачам. Використовуючи ці переваги, мережі 5G можуть забезпечити надійну та ефективну комунікаційну інфраструктуру.

Кілька сценаріїв ілюструють практичне впровадження формування променя в мережах 5G. У міських районах із високою щільністю користувачів формування променя може динамічно розподіляти ресурси для керування перевантаженням мережі та забезпечення безперебійного з'єднання [1]. Ця адаптивність також корисна в місцях проведення подій, де виникають тимчасові стрибки використання мережі, що дозволяє ефективно розподіляти ресурси. Крім того, у сільській місцевості формування променя розширює покриття мережі, охоплюючи користувачів у віддалених місцях із покращеною потужністю сигналу. Ці сценарії демонструють універсальність формування променя для вирішення різноманітних проблем мережі та оптимізації продуктивності в різних середовищах. Завдяки широкому діапазону використання, формування променя відіграє вирішальну роль в успішному розгортанні технології 5G.

Small Cells

Малі комірки є фундаментальним компонентом в архітектурі мобільних мереж 5G, відіграючи вирішальну роль у збільшенні пропускної здатності та покриття мережі. По суті, малі комірки відносяться до малопотужних вузлів стільникового радіодоступу, які працюють у діапазоні від 10 метрів до кількох кілометрів. Вони відіграють важливу роль у підтримці високочастотних діапазонів, що використовуються в 5G, які, пропонуючи вищі швидкості передачі даних, також мають менший радіус дії, ніж їхні низькочастотні аналоги. Розгортаючи малі стільники, мережеві оператори можуть ефективно керувати підвищеним попитом на дані та підключення, особливо в густонаселених районах. Ці комірки допомагають розвантажити трафік із традиційних макрокомірок, забезпечуючи безперебійне та високошвидкісне підключення користувачів [7].

Стратегії розгортання малих комірок суттєво відрізняються між міськими та сільськими середовищами, кожна з яких представляє унікальні можливості та виклики. У міських районах висока щільність будівель та інфраструктури забезпечує численні місця для встановлення невеликих комірок, наприклад, на

ліхтарних стовпах, стінах будівель та інших існуючих структурах. Таке щільне розгортання має вирішальне значення для вирішення проблеми високої щільності користувачів і забезпечення необхідної потужності та покриття. Навпаки, у сільській місцевості фокус зміщується на покриття більших географічних територій з меншою кількістю користувачів. Тут можна стратегічно розмістити малі стільники, щоб заповнити прогалини в охопленні, залишені макростільниками, гарантуючи, що навіть віддалені райони отримають переваги від прогресу технології 5G. Ці різні стратегії демонструють гнучкість і адаптивність розгортання малих клітинок для задоволення різноманітних вимог мережі [5].

Вплив малих стільників на ефективність мережі та покриття в мережах 5G є глибоким, що значно покращує обидва аспекти. Збільшуючи кількість точок доступу в мережі, малі комірки допомагають зменшити затримку та покращити пропускну здатність даних, роблячи мережу більш ефективною. Це особливо важливо в 5G, де низька затримка є критичною вимогою для багатьох додатків, включаючи автономні транспортні засоби та віддалені операції в режимі реального часу. Крім того, малі стільники сприяють кращому покриттю мережі, забезпечуючи послідовне обслуговування в складних умовах, наприклад усередині будівель або в густонаселених міських районах. Це покращене покриття не тільки покращує роботу користувачів, але й гарантує, що мережа може підтримувати широкий спектр пристроїв і програм, виконуючи одну з основних обіцянок технології 5G [8].

Edge Computing

Граничні обчислення представляють собою ключовий прогрес в архітектурі мобільних мереж 5G, докорінно змінюючи спосіб обробки та передачі даних. Завдяки децентралізації обробки даних ближче до джерела, периферійні обчислення зменшують залежність від централізованих центрів обробки даних [6]. Ця зміна особливо важлива в контексті 5G, який вимагає наднизької затримки та високошвидкісної передачі даних для підтримки різноманітних додатків, від автономних транспортних засобів до розумних міст. Крім того, периферійні

обчислення полегшують аналіз даних у реальному часі та прийняття рішень, підвищуючи загальну гнучкість і швидкість реагування мережі [9].

Таблиця 2.1.

Архітектурні особливості мобільних мереж 5G

Архітектурна особливість	Призначення	Переваги
Нарізка мережі (Network Slicing)	Дозволяє створювати кілька логічних мереж в одній фізичній інфраструктурі	Гнучкість, оптимізація ресурсів, адаптація під різні потреби
Масивний MIMO (Massive MIMO)	Збільшує пропускну здатність та покращує ефективність спектру	Збільшення кількості підключених пристроїв, підвищення продуктивності
Формування променя (Beamforming)	Спрямовує сигнал на конкретного користувача для покращення зв'язку	Зниження інтерференції, покращення пропускної здатності
Малі комірки (Small Cells)	Забезпечують розширене покриття та підвищену ємність	Покращення покриття, зменшення затримок
Граничні обчислення (Edge Computing)	Обробка даних ближче до джерела для зниження затримки	Швидка обробка даних, зниження навантаження на ядро мережі
Віртуалізація мережевих функцій (NFV)	Віртуалізація мережевих функцій для підвищення гнучкості	Швидке масштабування послуг, зниження витрат на інфраструктуру
Програмно-визначена мережа (SDN)	Централізоване управління мережею для оптимізації ресурсів	Гнучке управління мережею, ефективність розподілу трафіку

Архітектурна особливість	Призначення	Переваги
Технологія міліметрових хвиль (mmWave)	Використання високочастотного спектру для підвищення швидкості	Висока швидкість передачі, підтримка нових сервісів
Покращення безпеки	Забезпечення надійного захисту даних та інфраструктури	Захист конфіденційності даних, зменшення кіберзагроз

У результаті мережі 5G можуть ефективніше керувати експоненціальним зростанням трафіку даних, забезпечуючи безперебійне підключення та покращений досвід користувачів.

Однією з основних переваг периферійних обчислень у мережах 5G є їх здатність значно зменшувати затримку, що важливо для додатків, які потребують обробки даних у реальному часі. Обробляючи дані ближче до кінцевого користувача або пристрою, периферійні обчислення мінімізують час, необхідний для переміщення даних через мережу [10]. Це зменшення затримки є життєво важливим для таких програм, як віртуальна реальність, доповнена реальність і віддалена хірургія, де навіть мілісекунда затримки може вплинути на продуктивність і взаємодію з користувачем. Крім того, периферійні обчислення дозволяють більш ефективно використовувати мережеві ресурси, оскільки вони зменшують навантаження на базову мережу та оптимізують розподіл пропускної здатності [6]. Така ефективність не тільки підвищує швидкість і надійність послуг 5G, але й сприяє більш стійкій і масштабованій мережевій інфраструктурі.

Впровадження периферійних обчислень у мережах 5G відкриває безліч варіантів використання в різних галузях, демонструючи універсальність і трансформаційний потенціал цієї технології. У секторі охорони здоров'я, наприклад, периферійні обчислення можуть підтримувати телемедицину та віддалений моніторинг пацієнтів, забезпечуючи миттєвий аналіз даних і зворотний зв'язок [11]. В автомобільній промисловості це дозволяє розробляти інтелектуальні

транспортні системи, де транспортні засоби спілкуються один з одним та з інфраструктурою для підвищення безпеки та ефективності. Крім того, периферійні обчислення полегшують розгортання інтелектуальних виробничих процесів у промисловому секторі, дозволяючи здійснювати моніторинг у реальному часі та оптимізувати виробничі лінії [12]. Ці різноманітні додатки підкреслюють критичну роль периферійних обчислень у стимулюванні інновацій і розширенні можливостей мереж 5G у різних областях.

Віртуалізація мережевих функцій (NFV)

Віртуалізація мережевих функцій (NFV) — це трансформаційна концепція в архітектурі мобільних мереж 5G, спрямована на підвищення гнучкості та масштабованості шляхом відокремлення мережевих функцій від фірмового обладнання. У мережах 5G NFV дозволяє віртуалізувати основні функції мережі, дозволяючи їм працювати на стандартній обчислювальній інфраструктурі, а не на спеціальному обладнанні. Ця зміна полегшує керування мережею та швидке розгортання служб, оскільки функціональні можливості можна швидко створювати, масштабувати або змінювати за потреби. Роль NFV у 5G є ключовою, оскільки вона підтримує створення більш динамічного та програмованого мережевого середовища, яке має важливе значення для задоволення різноманітних вимог сучасних додатків, включаючи Інтернет речей (IoT) і наднадійну систему з низькою затримкою. комунікацій (URLLC) [1].

Однією із значних переваг віртуалізації мережевих функцій у 5G є підвищення ефективності керування мережею та її роботи. Використовуючи NFV, оператори можуть значно скоротити витрати, пов'язані з фізичною інфраструктурою, одночасно підвищуючи гнучкість надання мережевих послуг. Такий підхід не тільки зменшує потребу в значних інвестиціях у апаратне забезпечення, але також дозволяє оптимізувати мережу та розподілити ресурси в реальному часі. Можливість впроваджувати зміни в мережу шляхом оновлення програмного забезпечення, а не капітального ремонту апаратного забезпечення, сприяє створенню більш стійкої та гнучкої мережевої інфраструктури. Отже, така віртуалізація сприяє бездоганній інтеграції інноваційних технологій і послуг, тим

самим прискорюючи темпи технологічного прогресу та покращуючи досвід користувачів [13].

Незважаючи на численні переваги, реалізація віртуалізації мережевих функцій у мережах 5G створює певні проблеми, які необхідно вирішити. Однією з основних перешкод є забезпечення безпеки та надійності віртуалізованих середовищ, оскільки абстракція мережевих функцій може створити вразливі місця та збільшити площу атаки. Крім того, інтеграція NFV в існуючу мережеву архітектуру вимагає значних інвестицій з точки зору як часу, так і ресурсів, а також розвитку нових наборів навичок серед мережевих операторів. Крім того, досягнення сумісності між віртуалізованими функціями від різних постачальників може бути складним, що потребує стандартизованих інфраструктур і протоколів для забезпечення безперебійного зв'язку та функціональності. Вирішення цих проблем має вирішальне значення для успішного розгортання та роботи NFV у мережах 5G [14].

Програмно-визначена мережа (SDN)

Програмно-визначена мережа (SDN) відіграє ключову роль в архітектурі мобільних мереж 5G, пропонуючи революційний підхід до управління та проектування мережі. На відміну від традиційних мережевих архітектур, SDN відокремлює площину керування від площини даних, що дозволяє централізоване керування мережею та динамічний розподіл ресурсів [13]. Це розділення має вирішальне значення для 5G, оскільки воно сприяє бездоганній інтеграції з різними мережевими функціями та послугами, забезпечуючи адаптацію мережі до різноманітних вимог і умов. Інтегруючи SDN із 5G, оператори можуть створити більш гнучку та програмовану мережеву інфраструктуру, яка підтримує швидке розгортання нових послуг і функцій, покращуючи тим самим загальний досвід роботи з користувачем.

Інтеграція SDN у мережі 5G дає численні переваги, зокрема з точки зору керування мережею та гнучкості. Однією з головних переваг є можливість ефективніше керувати мережевим трафіком, що важливо для обробки величезних обсягів даних, створених послугами 5G [15]. SDN дозволяє операторам мереж

впроваджувати політики керування трафіком у реальному часі, оптимізуючи використання пропускної здатності та зменшуючи затримку. Крім того, можливість програмування SDN дозволяє легко налаштовувати мережеву поведінку відповідно до конкретних потреб додатків, забезпечуючи таким чином гнучке та чутливе мережеве середовище. Ця гнучкість є значною перевагою в підтримці різноманітних додатків, починаючи від розширеного мобільного широкосмугового зв'язку (eMBB) і закінчуючи наднадійним зв'язком із малою затримкою (URLLC).

Практичні застосування SDN в управлінні мережами 5G вже очевидні в різних випадках використання. Наприклад, SDN можна використовувати для оптимізації нарізки мережі, ключової функції 5G, яка дозволяє кільком віртуальним мережам співіснувати в спільній фізичній інфраструктурі [11]. Ця можливість гарантує, що різні служби, такі як пристрої Інтернету речей і високошвидкісний мобільний широкосмуговий зв'язок, отримають необхідні ресурси та якість обслуговування. Крім того, SDN полегшує розгортання периферійних обчислювальних рішень, покращуючи можливості обробки на межі мережі та зменшуючи затримку для чутливих до часу програм. Ці приклади ілюструють, як SDN не тільки покращує ефективність мережі, але й уможливлює інноваційні послуги та додатки, які використовують весь потенціал технології 5G.

Технологія міліметрових хвиль

Технологія міліметрових хвиль (mmWave) є ключовим прогресом у сфері мереж 5G, пропонуючи неперевершені можливості спектру, які підвищують як швидкість, так і пропускну здатність. Розуміння спектру mmWave передбачає заглиблення у діапазони високих частот, як правило, від 24 ГГц до 100 ГГц, які є вирішальними для досягнення надвисокої швидкості передачі даних, яка визначає мережі 5G [16]. Цей діапазон спектру дозволяє значно збільшити пропускну здатність, забезпечуючи високу швидкість передачі даних і підтримуючи величезну кількість підключених пристроїв одночасно. Здатність технології mmWave забезпечувати таку покращену продуктивність — це те, що робить її наріжним каменем інфраструктури 5G, знаменуючи суттєвий крок вперед у порівнянні з попередніми поколіннями технологій мобільних мереж.

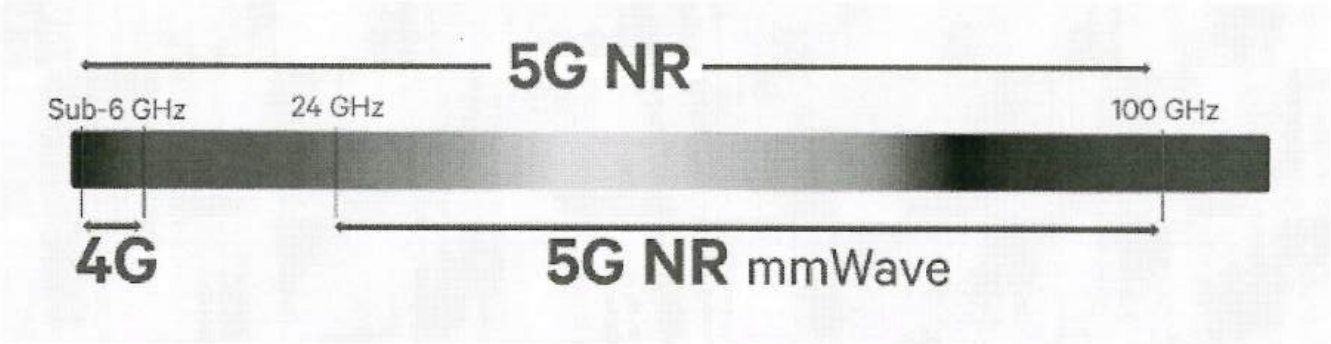


Рис. 2.3. Технологія міліметрових хвиль (mmWave)

Застосування технології міліметрових хвиль у мережах 5G є ключовим засобом високошвидкісного зв'язку з низькою затримкою, необхідного для сучасних мобільних додатків. Використовуючи спектр mmWave, мережі 5G можуть підтримувати вимогливі варіанти використання, такі як доповнена реальність (AR), віртуальна реальність (VR) і передові додатки IoT. Примітно, що наднизька затримка 5G, що підтримується mmWave, забезпечує безперебійну взаємодію в додатках у режимі реального часу, що важливо для критично важливих операцій, таких як віддалена медична допомога та автономне водіння [6]. Завдяки стратегічному впровадженню технології mmWave мережі 5G не тільки вдосконалюють традиційний мобільний зв'язок, але й прокладають шлях для інноваційних послуг і програм, які раніше були недоступні для мереж старих поколінь.

Незважаючи на багатообіцяючі можливості технології міліметрових хвиль у мережах 5G, її розгортання супроводжує кілька проблем. Однією з головних проблем є обмежений діапазон сигналів мм-хвиль, які схильні до значного загасання та можуть бути легко закриті фізичними перешкодами, такими як будівлі та дерева [3]. Це вимагає встановлення багатьох невеликих осередків для забезпечення постійного покриття, що може бути дорогим і складним з точки зору логістики. Крім того, сприйнятливість частот мм-хвиль до перешкод від факторів навколишнього середовища, таких як дощ і листя, створює додаткові технічні перешкоди, які необхідно вирішити. Подолання цих проблем має важливе значення

для повного використання потенціалу технології mmWave і забезпечення широкого впровадження та успіху мереж 5G.

2.2. Можливості та переваги використання 5G в Розумному Місті

Покращення якості зв'язку

Поява технології 5G віщує революцію в пропускній здатності мережі, особливо в розумних містах, де продовжує зростати попит на додатки, що інтенсивно передають дані. Одне з найбільш значних удосконалень, які пропонує 5G, — це його збільшена пропускна здатність, яка, за оцінками, у десять разів перевищує пропускну здатність мереж 4G [1]. Це суттєве збільшення пропускної здатності сприяє швидшій швидкості передачі даних, дозволяючи розумним містам безперебійно підтримувати безліч підключених пристроїв і послуг. Більша пропускна здатність мереж 5G означає, що більше користувачів можуть отримати доступ до високошвидкісного Інтернету одночасно, не відчуваючи зниження продуктивності. Це критично важливо в міському середовищі, де висока щільність населення та цифрова активність.

Ще однією головною перевагою технології 5G є її здатність мінімізувати затримку, що має вирішальне значення для ефективного функціонування розумних міст. Зменшення затримок у мережі в першу чергу пов'язано з передовою інфраструктурою 5G, яка працює на вищих частотах і підтримує швидший обмін даними [2]. Низька затримка є важливою для додатків у реальному часі, таких як автономні транспортні засоби, дистанційні послуги охорони здоров'я та розумні системи керування трафіком. Забезпечуючи мінімальну затримку, технологія 5G дозволяє розумним містам впроваджувати інноваційні рішення, які вимагають миттєвої обробки даних і відповіді. Ця можливість не тільки підвищує ефективність роботи, але й сприяє покращенню безпеки та досвіду користувачів у міських умовах.

Надійність з'єднання – це ще одна сфера, де технологія 5G перевершує своїх попередників, пропонуючи більш надійну мережу для мешканців розумних міст і послуг. Підвищена надійність є результатом здатності 5G працювати на кількох діапазонах частот, що забезпечує послідовне підключення навіть у зонах із високим перевантаженням мережі [3]. Крім того, мережі 5G створені для підтримки стабільного з'єднання, незважаючи на наявність багатьох підключених пристроїв, що є поширеним сценарієм у розумних містах. Ця підвищена надійність життєво важлива для критично важливих додатків, таких як служби екстреної допомоги, операції з громадською безпекою та управління основною громадською інфраструктурою, де безперебійне з'єднання може істотно змінити результати.

Інтернет речей (IoT) у Розумному Місті

Масштабованість підключення пристроїв є головною перевагою 5G у сфері IoT у розумних містах. На відміну від своїх попередників, 5G підтримує підвищену щільність з'єднання, дозволяючи підключати значно більшу кількість пристроїв на одиницю площі, що має вирішальне значення для експансивного зростання додатків IoT [4]. Цей прогрес гарантує, що різні компоненти розумного міста, такі як світлофори, камери спостереження та системи громадського транспорту, можуть безперешкодно спілкуватися та обмінюватися даними. Крім того, гнучкі форми сигналів 5G і нові розподіли спектру забезпечують надійну основу для інноваційних рішень IoT, що дозволяє містам ефективно керувати мережами своїх пристроїв і розширювати їх за потреби [5]. Ця масштабованість має важливе значення для забезпечення постійного припливу нових пристроїв IoT, забезпечуючи зв'язану екосистему, яка покращує міське життя.

Оптимізація споживання енергії є ще однією важливою перевагою інтеграції 5G з IoT у розумних містах. Висока енергоефективність мереж 5G є значним покращенням у порівнянні з попередніми поколіннями, зменшуючи енергоспоживання підключених пристроїв [3]. Ця функція особливо корисна для пристроїв IoT з живленням від акумуляторів, таких як датчики та інтелектуальні лічильники, які можуть працювати довше без частих підзарядок або замін. Крім того, сегментація мережі в 5G сприяє оптимізації енергоспоживання шляхом

створення підмереж, які надають пріоритет енергоефективним операціям, тим самим мінімізуючи витрати [1]. Як наслідок, розумні міста можуть досягти сталого використання енергії, додатково сприяючи екологічним цілям і знижуючи експлуатаційні витрати.



Рис. 2.4. Переваги використання 5G в Розумному Місті

Інтеграція 5G з інтелектуальними датчиками є кардинальною розробкою для розумних міст, яка підвищує загальну ефективність і ефективність міських систем. Завдяки можливості 5G підтримувати величезну кількість датчиків і пристроїв, міста можуть здійснювати моніторинг у реальному часі та збір даних у різних інфраструктурах [6]. Ця інтеграція дозволяє точно контролювати та управляти міськими ресурсами, що призводить до покращення надання послуг та використання ресурсів. Крім того, оперативне реагування в режимі реального часу

завдяки 5G гарантує, що інтелектуальні датчики можуть оперативно реагувати на зміни в навколишньому середовищі, полегшуючи негайне коригування та втручання за потреби [7]. Отже, розгортання інтелектуальних датчиків на основі 5G дозволяє містам працювати більш розумно та проактивно, забезпечуючи мешканцям безперебійний та оптимізований міський досвід.

Транспортні системи

Поява технології 5G має потенціал для революції в автономних транспортних системах у розумних містах. Завдяки швидкості передачі даних, яка в 10 разів перевищує швидкість 4G, досягаючи теоретичної швидкості до 10 Гбіт/с, 5G може значно розширити можливості автономних транспортних засобів [8]. Незважаючи на те, що автономні автомобілі повинні мати можливість працювати без постійного підключення до мережі, висока швидкість передачі даних і низька затримка мереж 5G забезпечують зв'язок у режимі реального часу між транспортними засобами та інфраструктурою. Це забезпечує більш ефективну навігацію та покращує заходи безпеки, оскільки транспортні засоби можуть отримувати актуальну інформацію про дорожній рух і відповідним чином реагувати. Крім того, здатність 5G працювати з високою щільністю підключених пристроїв гарантує, що автономні транспортні засоби можуть безперебійно взаємодіяти з іншими компонентами розумного міста, такими як світлофори та дорожні датчики, сприяючи більш інтегрованій та ефективній транспортній екосистемі.

Інтелектуальні транспортні системи (ITS) отримають величезну користь від впровадження технології 5G у розумних містах. Виняткова продуктивність 5G у комунікаційних програмах дозволяє бездоганно інтегрувати різні компоненти ITS, тим самим підвищуючи їх загальну ефективність [9]. Завдяки здатності підтримувати високу щільність датчиків і забезпечувати надійне підключення в різних сценаріях мережі 5G дозволяють аналізувати дані в реальному часі та приймати рішення в рамках ITS. Це включає в себе можливість керувати та оптимізувати маршрути громадського транспорту, зменшувати затори та покращувати координацію служб екстреного реагування. Крім того, надійність і швидкість 5G сприяють розгортанню передових технологій, таких як системи

управління трафіком на основі штучного інтелекту, які можуть аналізувати величезні обсяги даних для прогнозування та усунення вузьких місць трафіку, забезпечуючи більш плавне та ефективне пересування в межах міста.

Ефективний моніторинг і управління дорожнім рухом є ключовим аспектом розвитку розумного міста, і технологія 5G відіграє ключову роль у досягненні цієї мети. Вищі швидкості передачі даних і зниження перевантаженості мережі, що забезпечується 5G, дозволяють розгортати передові рішення для моніторингу, які можуть фіксувати та аналізувати дані трафіку майже в реальному часі [1]. Ця можливість дозволяє міській владі швидко реагувати на дорожні події, коригувати сигнали світлофора для оптимізації руху та надавати водіям своєчасну інформацію про дорожні умови. Крім того, інтеграція 5G з пристроями IoT, такими як камери та датчики, дозволяє безперервно контролювати дорожню інфраструктуру, допомагаючи в обслуговуванні та ремонті доріг до того, як виникнуть значні проблеми. Таким чином, впровадження 5G в системи управління дорожнім рухом не тільки покращує ефективність міського транспорту, але й підвищує безпеку та стійкість розумних міст.

Розумна енергетика

Впровадження технології 5G в інтелектуальні системи управління енергією пропонує трансформаційний підхід до управління споживанням енергії в міському середовищі. Ці системи розроблені для підтримки великої кількості недорогих пристроїв, розподілених на великих територіях, забезпечуючи наднизьке енергоспоживання, що є ключовим компонентом ефективного управління енергією в розумних містах [10]. Завдяки здатності 5G передавати дані на коротших довжинах хвиль, існує підвищена точність керування напрямком, що забезпечує відповіді в реальному часі та мінімальну затримку [7]. Така підвищена ефективність не тільки зменшує витрати на енергоспоживання, але й покращує роботу та надійність комунальних послуг. Розширені можливості підключення та швидка обробка даних 5G сприяють розробці інтелектуальних систем управління ресурсами, які можуть динамічно коригувати моделі споживання енергії відповідно до вимог реального часу [11].

Таблиця 2.2.

Порівняння технологій 4G та 5G

Параметр	4G	5G
Максимальна швидкість передачі даних	До 1 Гбіт/с	До 10 Гбіт/с
Затримка (Latency)	20-50 мс	1-5 мс
Пропускна здатність	Нижча	Вища
Щільність підключень	100 000 пристроїв на км²	Мільйон пристроїв на км²
Ефективність спектру	Менш ефективний	Вища ефективність
Архітектура мережі	Монолітна	Модульна, з підтримкою SDN/NFV
Частотний діапазон	1-6 ГГц	До 100 ГГц (мм-хвилі)
Енергоспоживання	Високе	Знижене
Підтримка IoT	Обмежена	Повна підтримка
Безпека	Базові механізми шифрування	Розширені механізми безпеки

Інтеграція технології 5G з відновлюваними джерелами енергії має ключове значення для оптимізації розподілу енергії в розумних містах. Децентралізований характер відновлюваних джерел енергії, таких як сонце та вітер, вимагає надійної комунікаційної мережі для ефективної інтеграції та розподілу [12]. Мережі 5G забезпечують це, пропонуючи високошвидкісні надійні з'єднання, які забезпечують безперебійний зв'язок між розподіленими енергетичними ресурсами та мережею. Ця інтеграція дозволяє створити більш стійку енергетичну екосистему, зменшуючи залежність від невідновлюваних джерел і мінімізуючи вуглецеві сліди. Крім того, 5G покращує здатність відстежувати та контролювати потоки енергії, забезпечуючи ефективне використання та використання відновлюваної енергії. Завдяки вдосконаленій аналітиці даних і моніторингу в

реальному часі розумні міста можуть оптимізувати споживання та зберігання енергії, створюючи більш стійке та екологічно чисте міське середовище.

Оптимізація мереж передачі енергії в розумних містах значно підкріплюється можливостями технології 5G. Завдяки своїй здатності обробляти величезні обсяги даних з високою швидкістю та низькою затримкою, 5G сприяє безперебійній роботі складних енергетичних мереж [13]. Цей новий стандарт зв'язку забезпечує широкий спектр зв'язків від виробництва до розподілу, забезпечуючи ефективну передачу енергії між міськими районами. Можливості сегментації мережі зменшують перевантаження, забезпечуючи швидшу передачу даних і більш надійний розподіл енергії [1]. Використовуючи 5G, розумні міста можуть впроваджувати розширені стратегії управління електромережами, які передбачають і реагують на коливання попиту на енергію, тим самим підвищуючи стабільність і надійність електропостачання. Зрештою, це сприяє створенню більш сталої та ефективної енергетичної інфраструктури, що відповідає головним цілям розвитку розумного міста.

Безпека та моніторинг

Впровадження технології 5G значно розширило можливості відеоспостереження в реальному часі в розумних містах. Завдяки неперевершеній високій швидкості передачі даних і низькій затримці 5G забезпечує безперебійну потокову передачу відео високої чіткості навіть у густонаселених міських районах [14]. Цей прогрес дозволяє ефективніше контролювати громадські місця та керувати ними, підвищуючи загальну безпеку. Можливість без затримки передавати відео в реальному часі забезпечує ситуаційну обізнаність у режимі реального часу для правоохоронних та екстрених служб, сприяючи швидшому часу реагування та кращому прийняттю рішень. Крім того, інтеграція 5G з існуючими системами відеоспостереження забезпечує надійну інфраструктуру, яка підтримує масштабоване та гнучке розгортання в різних міських середовищах [15].

Технологія 5G також відіграє вирішальну роль у розробці складних систем виявлення аномалій і загроз у розумних містах. Розширені можливості мережі дозволяють ефективно обробляти та аналізувати великі обсяги даних, зібраних з

різних датчиків і пристроїв [16]. Цей підхід на основі даних дозволяє ідентифікувати незвичайні закономірності та потенційні загрози в реальному часі, тим самим підвищуючи стійкість міста до проблем безпеки. Наприклад, раптове збільшення навантаження на мережу може бути виявлено негайно, сигналізуючи про потенційні кіберзагрози або збої в роботі системи [17]. Такі проактивні рішення моніторингу не тільки зміцнюють безпеку міського середовища, але й покращують загальну якість життя, забезпечуючи безперебійну роботу основних служб.

Оскільки міста продовжують розвиватися в розумне середовище, важливість кібербезпеки в мережевій інфраструктурі неможливо переоцінити. Розгортання мереж 5G відкриває нові можливості для управління та захисту даних, що передаються через різні платформи [18]. Він забезпечує розширені функції безпеки, такі як покращені протоколи шифрування та нарізка мережі, які гарантують збереження цілісності та конфіденційності даних. Крім того, гнучкість мереж 5G дозволяє створювати індивідуальні рішення безпеки, які можуть адаптуватися до унікальних вимог різних програм і послуг [19]. Ця адаптивність має вирішальне значення для захисту конфіденційної інформації та підтримки довіри громадян до цифрової інфраструктури, яка лежить в основі ініціатив розумного міста.

РОЗДІЛ 3. МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІНФРАСТРУКТУРІ РОЗУМНОГО МІСТА З ВИКОРИСТАННЯМ 5G

3.1. Аналіз загроз та вразливостей в інфраструктурі Розумного Міста на основі 5G

Загрози мережевої інфраструктури

Атаки на базовій станції є однією з найсерйозніших загроз для мережевої інфраструктури розумних міст, що використовують технологію 5G. Базові станції запускають вузли в мережі, забезпечуючи зв'язок між мобільними пристроями та центральною мережею. Це робить їх головною метою для кібератаків, які можуть мати різні форми, такі як фізичні атаки або втручання в роботу програмного забезпечення [1]. Поразка базових станцій може призвести до серйозних наслідків, включаючи втрату зв'язку, зниження якості обслуговування, а також злам конфіденційних даних. Для мінімізації цих ризиків необхідно передбачити заходи щодо захисту базових станцій, таких як посилення фізичної безпеки, а також застосування методів захисту від кібератаків, включаючи шифрування трафіку та систему постійного моніторингу [2].

Перехоплення трафіку та несанкціонований доступ є іншими вагомими загрозами для інфраструктури розумних міст на базі 5G. Збільшення обсягу даних, що передаються через 5G-мережу, робить їх привабливими для зловмисників, які хочуть отримати доступ до конфіденційної інформації або порушити нормальну роботу системи [3]. Такі атаки можуть бути здійснені за допомогою різних методів, включаючи використання шкідливого програмного забезпечення або використання експлуатаційних уразливостей у мережевих протоколах. Щоб зменшити ризики, пов'язані з перехопленням трафіку та несанкціонованим доступом, необхідно впроваджувати сильні системи аутентифікації, шифрування даних і розподілені системи виявлення вторгнень [4].

Вразливість мережевих протоколів є ще однією суттєвою проблемою безпеки в інфраструктурі розумних міст. 5G-мережі містяться на складних протоколах для

забезпечення швидкого та надійного зв'язку, але ці протоколи можуть бути пов'язані з вразливістю, яка може бути використана зловмисниками для здійснення атак [5]. Наприклад, недоліки в протоколах аутентифікації можуть дозволити злочинцям отримати доступ до мережі та маніпулювати переданими даними. Щоб протидіяти цим загрозам, розробники мають регулярно переглядати та оновлювати протоколи безпеки, а також забезпечувати їх відповідність новітнім стандартам безпеки [6].

Таблиця 3.1.

Аналіз загроз та вразливостей в інфраструктурі Розумного Міста на основі 5G

Параметр	Основні загрози	Заходи безпеки
Загрози мережевої інфраструктури	Атаки на базові станції, перехоплення трафіку, вразливість протоколів	Шифрування, аутентифікація, моніторинг
Кіберзагрози Інтернету речей (IoT)	DDoS-атаки, недостатність автентифікації, неконтрольований доступ	Захищені протоколи, багаторівнева аутентифікація, контроль доступу
Уразливості систем управління трафіком	Маніпуляція даними, підміна маршрутів, перехоплення інформації	Шифрування, захищені маршрутизаційні алгоритми, аналіз аномалій
Ризики для критичної інфраструктури	Атаки на енергомережі, вразливість водопостачання, саботаж систем	Резервування, моніторинг, багаторівнева система захисту
Вплив соціальної інженерії	Фішинг, маніпулювання даними, злом облікових записів	Навчання персоналу, багатофакторна аутентифікація, моніторинг доступу

Параметр	Основні загрози	Заходи безпеки
Уразливості кіберфізичних систем	Злам систем безпеки, втручання в датчики, збої автоматизованих систем	Інтеграція безпеки IoT, захищені шлюзи, аудит безпеки
Загрози конфіденційності даних	Несанкціонований збір даних, витік через ненадійні канали, використання великих даних	Політики захисту, шифрування, контроль доступу
Вразливості мобільних додатків	Ін'єкційні атаки, незахищені API, підробка транзакцій	Регулярні оновлення, аудит, захист API
Вплив атак на громадський транспорт	Спуфінг, несанкціоноване управління, маніпуляція тарифами	Верифікація сигналів, контроль доступу, шифрування даних

Кіберзагрози Інтернету речей (IoT)

Масові розподілені атаки на відмову в обслуговуванні (DDoS) через пристрої IoT становлять значну загрозу для інфраструктури розумного міста. Ці атаки використовують величезну кількість взаємопов'язаних пристроїв, щоб перевантажити мережеві ресурси, викликаючи збої в основних службах, таких як управління трафіком, охорона здоров'я та системи громадської безпеки [7]. Велика кількість пристроїв IoT у розумних містах, від вуличних ліхтарів до камер спостереження, пропонує кіберзлочинцям численні точки входу для здійснення таких атак. Цей потенціал для масштабних збоїв підкреслює необхідність надійних заходів безпеки та моніторингу в реальному часі для зменшення ризику DDoS-атак. Відсутність стандартизації пристроїв IoT ще більше ускладнює реалізацію єдиних протоколів безпеки, роблячи ці системи особливо вразливими для експлуатації.

Недостатність механізмів автентифікації в пристроях IoT створює ще одну критичну вразливість в інфраструктурах розумних міст. Багато пристроїв IoT не мають розширених протоколів автентифікації, що робить їх сприйнятливими до несанкціонованого доступу та контролю з боку зловмисників [8]. Неналежна

автентифікація може призвести до несанкціонованого доступу до даних, маніпуляцій і навіть фізичної шкоди, якщо критичні системи скомпрометовані. Ефективна автентифікація життєво важлива для того, щоб лише уповноважені особи могли спілкуватися з цими пристроями, тим самим захищаючи конфіденційну інформацію та зберігаючи цілісність операцій у розумному місті. Посилення процесів автентифікації вимагає інтеграції багатофакторної автентифікації та розробки безпечних, масштабованих рішень, які можна однаково застосовувати на різноманітних пристроях Інтернету речей.

Неконтрольований доступ до критично важливих систем у мережах IoT ще більше посилює ризики кібербезпеки, з якими стикаються розумні міста. Якщо пристрої IoT не захищені належним чином, вони можуть служити шлюзами для зловмисників, щоб проникнути та маніпулювати критично важливими системами, що потенційно може спричинити повсюдний хаос [1]. Наприклад, зловмисник, отримавши доступ до міської системи керування дорожнім рухом, може спричинити серйозні перебої в русі та поставити під загрозу громадську безпеку. Складність і взаємопов'язаність систем «розумного міста» вимагають суворого контролю доступу та впровадження всебічної системи безпеки. Важливо встановити чіткі вказівки та політику щодо керування доступом, гарантуючи, що лише авторизований персонал може взаємодіяти з конфіденційними системами. Регулярні аудити та оцінки вразливостей мають вирішальне значення для виявлення та пом'якшення потенційних прогалин у безпеці в цих складних середовищах.

Уразливості систем управління трафіком

Розумна міська інфраструктура, яка значною мірою залежить від технології 5G, стикається зі значною вразливістю в системах управління трафіком, зокрема через маніпуляції даними трафіку. Ці системи, які є невід'ємною частиною підтримки безперебійних транспортних процесів, можуть бути скомпрометовані зловмисниками, які змінюють дані про дорожній рух, створюючи затори та навіть аварії [9]. Взаємопов'язаний характер розумних міст робить такі системи дуже сприйнятливими до кіберзагроз, оскільки дані з датчиків і пристроїв Інтернету

речей безперервно обмінюються для моніторингу та керування потоком трафіку [10]. Змінений потік даних може призвести до неправильного прогнозування дорожнього руху та маршрутизації, порушуючи щоденні поїздки та екстрені служби. Ці маніпуляції можуть мати каскадні наслідки, не лише впливаючи на транспортну систему, але й спричиняючи економічні та операційні збої в місті. Оскільки міста ростуть і стають більш залежними від цих технологій, усунення цих вразливостей стає критично важливим для забезпечення безпеки та ефективності міських транспортних мереж.

Окрім маніпулювання даними, розумні міські транспортні системи вразливі до підробки сигналів і маршрутів, що може серйозно порушити міську мобільність. Перехоплюючи та змінюючи сигнали світлофора, кіберзловмисники можуть перенаправляти або затримувати трафік, створюючи загрозу громадській безпеці та ефективності [5]. Атаки підробки можуть бути організовані, щоб змінити послідовність світлофорів, вводячи водіїв в оману та потенційно спричиняючи аварії. Такі вразливі місця виявляють крихкість міської інфраструктури, де залежність від цифрових систем може бути використана для ініціювання повсюдного хаосу. Перехід до мереж 5G посилює ці ризики через збільшення зв'язку та обміну даними, що вимагає надійних заходів безпеки для виявлення та запобігання таким атакам. Забезпечення цілісності сигнального зв'язку та встановлення безпечних протоколів маршрутизації є життєво важливими кроками для захисту інфраструктури розумного міста від цих загроз.

Ще однією критичною вразливістю в системах керування дорожнім рухом у розумних містах є перехоплення інформації про транспорт, що може призвести до несанкціонованого доступу до конфіденційних даних. Кіберзлочинці можуть використовувати ці слабкі сторони для збору інформації про рух транспортних засобів і схеми дорожнього руху, що потенційно може призвести до вторгнення в конфіденційність і цілеспрямованих атак [11]. Постійний моніторинг і розширений аналіз даних необхідні для виявлення та пом'якшення потенційних порушень, що дозволяє міській владі контролювати ці процеси. Використовуючи автоматизовані рішення для виявлення загроз на основі штучного інтелекту, міста можуть

покращити свою здатність прогнозувати кіберзагрози та реагувати на них [12]. Ці рішення покладаються на складні алгоритми для обробки величезних обсягів даних, гарантуючи швидке виявлення та усунення будь-яких аномалій. Оскільки розумні міста продовжують розвиватися, пріоритетність кібербезпеки в системах управління трафіком є ключовою для захисту як інфраструктури, так і громадян, які від неї залежать.

Ризики для критичної інфраструктури

Атаки на енергомережі міста становлять значну загрозу для критичної інфраструктури розумних міст. Оскільки енергомережі все більше інтегруються з технологіями 5G, вони залишаються більш вразливими до кіберзагроз, які можуть призвести до масштабних відключень електроенергії. такі атаки можуть бути здійснені через зловмисні програми, які проникають в систему управління енергопостачанням і змінюють параметри роботи. Це може збільшити короткі замкнення або навіть повні аварії трансформаторів [1]. З огляду на важливість електропостачання для забезпечення безперебійної роботи міста, такі збої можуть мати катастрофічні наслідки для безпеки та добробуту жителів.

Вразливість систем водопостачання також є критичним питанням у контексті безпеки розумних міст. Ці системи, оснащені сенсорами та контролерами, підключеними до Інтернету, можуть бути об'єктом кібератаку, який порушує їх роботу. Наприклад, зловмисники можуть перехоплювати дані з сенсорів або вводити в оману системи, щоб змінити параметри подачі води, що може призвести до забруднення або перерви у водопостачання [13]. Крім того, ризики для водопостачання посилилися через недостатню захист від нападу на віддалене управління, що може дозволити зловмисникам маніпулювати системами без фізичного доступу.

Саботаж розумних систем управління є ще однією суттєвою загрозою для критичної інфраструктури розумних міст. Такі системи, як світлофорні мережі, управління трафіком та громадським транспортом, значною мірою залежать від точності й своєчасності обміну даними. Зловмісники можуть маніпулювати цими даними, що призведе до хаосу на дорогах або збоїв у роботі громадського

транспорту [14]. Це підкреслює необхідність розробки ефективних стратегій захисту, здатних виявляти та запобігати таким загрозам, забезпечуючи при цьому безпеку та ефективність управління міськими ресурсами.

Вплив соціальної інженерії

Фішингові атаки становлять значну загрозу для жителів розумних міст, використовуючи людську психологію та довіру для отримання несанкціонованого доступу до конфіденційної інформації. Ці атаки часто маскуються під законні повідомлення від довірених організацій, змушуючи людей мимоволі ділитися конфіденційними даними, такими як паролі та фінансові деталі [15]. У контексті розумного міста, де переважає цифрова взаємодія, вплив фішингових атак може бути руйнівним, що призведе до компрометації персональних і муніципальних систем. Наслідки поширюються не тільки на окремих жертв, оскільки скомпрометовані облікові записи можуть служити шлюзами для подальшого проникнення в критичну інфраструктуру міста.

Маніпулювання особистими даними є ще одним критичним аспектом соціальної інженерії, який може підірвати інфраструктуру розумного міста. Зловмисники можуть використовувати вразливі місця в механізмах захисту даних, щоб змінити або зловживати особистою інформацією, що призведе до серйозних порушень конфіденційності та потенційної крадіжки особистих даних [1]. Наслідки таких маніпуляцій є далекосяжними, впливаючи не лише на залучених осіб, а й на цілісність загальноміських систем даних. У розумних містах, де прийняття рішень на основі даних має першочергове значення, викривлення інформації може призвести до погіршення процесу прийняття рішень і неоптимального розподілу ресурсів, що зрештою вплине на ефективність і безпеку міських послуг.

Злом облікових записів міських служб представляє величезний виклик для розумного управління містом, оскільки він включає як технічну майстерність, так і стратегічне маніпулювання методами соціальної інженерії. Кіберзлочинці можуть використовувати комбінацію атак грубої сили та стратегій фішингу, щоб отримати доступ до цих облікових записів, згодом порушуючи основні послуги та потенційно загрожуючи громадській безпеці [16]. Наслідки таких порушень

багатогранні: від збоїв у роботі до фінансових втрат і ерозії суспільної довіри до цифрових інфраструктур. Оскільки розумні міста продовжують значною мірою покладатися на взаємопов'язані системи, захист цих облікових записів стає обов'язковим для підтримки безперебійного функціонування міських послуг.

Уразливості кіберфізичних систем

Системи безпеки будівель є невід'ємною частиною інфраструктури розумного міста, і їх вразливість може мати далекосяжні наслідки. Впровадження технології 5G, покращуючи підключення та швидкість, створює нові ризики, які можуть поставити під загрозу ці системи. Наприклад, несанкціонований доступ до систем безпеки будівлі може призвести до вимкнення сигналізації або камер спостереження, створюючи можливості для фізичного проникнення. Ця вразливість посилюється взаємопов'язаною природою мереж 5G, де порушення в одному вузлі може мати каскадний вплив на інші підключені системи. Оскільки міста стають все більш залежними від розумних технологій, забезпечення надійних заходів кібербезпеки для побудови систем має вирішальне значення для запобігання потенційним загрозам і підтримки безпеки міського середовища [1].

Неконтрольоване втручання в роботу датчиків є ще однією критичною вразливістю інфраструктури розумного міста, особливо з впровадженням мереж 5G. Датчики відіграють життєво важливу роль у моніторингу та управлінні міськими операціями, від контролю руху до моніторингу навколишнього середовища. Однак розширені можливості підключення та передачі даних 5G можна використовувати для маніпулювання даними датчиків, що призводить до неточних показань і прийняття неправильних рішень. Наприклад, втручання в датчики руху може призвести до заторів або аварій через надання неправдивої інформації системам керування дорожнім рухом. Можливість порушувати дані датчиків без фізичного доступу підкреслює потребу в розширених протоколах безпеки для захисту цих основних компонентів інфраструктури розумного міста [3].

Порушення роботи автоматизованих систем у розумних містах створює значні ризики, особливо в контексті технології 5G. Автоматизовані системи,

наприклад ті, що керують громадським транспортом або розподілом енергії, значною мірою покладаються на дані в реальному часі та безперебійний зв'язок для ефективного функціонування. Атака на ці системи може призвести до повсюдного хаосу, вплинувши на тисячі жителів і потенційно завдавши шкоди основним міським службам. Інтеграція мереж 5G, пропонуючи покращену продуктивність, також створює вразливості, які необхідно усунути, щоб запобігти таким збоям. Забезпечення стійкості та безпеки автоматизованих систем є життєво важливим для підтримки функціональності та надійності роботи розумного міста [17].

Загрози конфіденційності даних

Швидке розширення інфраструктури розумного міста, якому сприяють мережі 5G, викликало серйозні занепокоєння щодо несанкціонованого збору персональних даних. Оскільки датчики та пристрої Інтернету речей поширюються в міському середовищі, обсяг даних, що генеруються, зростає експоненціально, підвищуючи ризик збору особистої інформації без згоди користувача. Цей несанкціонований збір даних становить суттєву загрозу конфіденційності особи, оскільки може включати конфіденційну інформацію, таку як місцезнаходження, звички та поведінка. Відсутність суворих правил захисту даних і можливість використання зловмисниками посилюють ці ризики [5]. Тому вкрай важливо встановити надійні рамки безпеки для захисту персональних даних у розумних містах.

Витік інформації через ненадійні канали є ще однією значною вразливістю в екосистемі розумного міста. Коли дані передаються між пристроями та центральними системами, вони часто перетинають незахищені мережі, що робить їх сприйнятливими до перехоплення та несанкціонованого доступу. Це може призвести до розголошення конфіденційних даних, що призведе до порушення конфіденційності та крадіжки особистих даних. Неадекватні протоколи шифрування та автентифікації ще більше ускладнюють цю проблему, роблячи дані вразливими для кібератак [18]. Щоб пом'якшити ці ризики, вкрай важливо запровадити захищені канали зв'язку, гарантуючи, що дані зашифровані та захищені на всіх етапах передачі.

Використання великих даних у розумних містах створює унікальний набір ризиків, зокрема щодо конфіденційності та безпеки даних. Хоча аналітика великих даних може запропонувати цінну інформацію для міського планування та управління, агрегування великих наборів даних може ненавмисно наражати людей на порушення конфіденційності. Можливість робити перехресні посилання та аналізувати дані з різних джерел може призвести до ненавмисних висновків про людей, таким чином ставлячи під загрозу їх конфіденційність [19]. Крім того, величезний обсяг зібраних даних створює труднощі для підтримки цілісності даних і забезпечення їх використання лише за призначенням. Таким чином, існує нагальна потреба створити всеохоплюючі структури управління даними, які б усунули ці ризики та забезпечили відповідальне використання великих даних у розумних міських середовищах.

Вразливості мобільних додатків для міських послуг

Ін'єкційні атаки та експлойти представляють значні вразливості в мобільних додатках, розроблених для міських служб. Ці атаки часто використовують такі методи, як ін'єкції SQL і міжсайтові сценарії (XSS), щоб маніпулювати даними та функціями програми, що може призвести до несанкціонованого доступу та витоку даних [20]. У контексті розумного міста, де численні програми спілкуються через мережі 5G, потенціал для таких типів атак зростає експоненціально. Завдяки інтеграції різних служб, таких як громадський транспорт і муніципальні служби, успішна ін'єкційна атака може порушити основні функції міста. Щоб пом'якшити ці ризики, вкрай важливо прийняти надійні заходи безпеки, включаючи регулярні перевірки коду та впровадження суворих процесів перевірки вхідних даних.

Незахищені інтерфейси API є ще однією критичною вразливістю мобільних додатків для міських послуг, особливо в розумному міському середовищі. API необхідні для з'єднання різних компонентів і сервісів, але коли вони недостатньо захищені, вони стають основними цілями для кібератак [1]. Зловмисники можуть використовувати ці інтерфейси для отримання несанкціонованого доступу до конфіденційної інформації або для виконання зловмисних команд, потенційно скомпрометувавши всю інфраструктуру розумного міста. Широке використання

API у «розумних» містах із підтримкою 5G посилює ризик, що робить обов'язковим впровадження протоколів безпеки, таких як автентифікація, шифрування та регулярні перевірки безпеки, щоб захистити ці інтерфейси від потенційних загроз.

Ризик підробки транзакцій і доступу в мобільних додатках для міських служб становить значну загрозу безпеці розумного міста. Зловмисники можуть маніпулювати процесами транзакцій або отримати неавторизований доступ, використовуючи вразливі місця в додатку або базових системах [1]. Це може призвести до шахрайських дій, таких як несанкціоновані фінансові операції або маніпулювання доступом до послуг, що може мати серйозні наслідки як для роботи міста, так і для його жителів. Для боротьби з цими загрозами важливо використовувати передові заходи безпеки, такі як багатофакторна автентифікація, технологія блокчейн для перевірки транзакцій і постійний моніторинг цілісності транзакцій, щоб переконатися, що всі дії є законними та безпечними.

3.2. Методи забезпечення кібербезпеки на основі мобільних мереж п'ятого покоління

Захист мережевої інфраструктури

Впровадження шифрування даних є фундаментальною стратегією захисту мережевої інфраструктури в мобільних мережах п'ятого покоління. Шифрування служить надійним бар'єром проти несанкціонованого доступу, гарантуючи, що будь-які перехоплені дані залишаються незрозумілими для потенційних зловмисників. Це надзвичайно важливо для захисту конфіденційної інформації, що передається через мережу, наприклад особистих даних користувачів і конфіденційних повідомлень. Застосовуючи розширені алгоритми шифрування, мережі 5G можуть підтримувати високий рівень безпеки, що важливо, враховуючи їхню збільшену пропускну здатність і більш широкий спектр частот, які вони

використовують [1]. Це гарантує збереження цілісності та конфіденційності даних, навіть якщо дані переміщуються з безпрецедентною швидкістю та обсягом.

Таблиця 3.2.

Основні інструменти кібербезпеки для захисту 5G-мереж

Ланка 5G мережі	Основні загрози	Методи захисту
Радіомережа (RAN)	Перехоплення сигналу, DDoS-атаки	Шифрування сигналів, аутентифікація
Транспортна мережа	Перехоплення трафіку, маніпуляція даними	Шифрування даних, захищені тунелі
Ядерна мережа (Core Network)	Несанкціонований доступ, шкідливе ПЗ	Моніторинг аномалій, багаторівнева автентифікація
Пристрій користувача (UE)	Фізичний доступ, фішинг	Багатофакторна автентифікація, біометрія
Оркестрація та управління	Неавторизоване втручання, експлуатація вразливостей	Сегментація доступу, політики безпеки
Міжмережеві з'єднання	Перехоплення даних, атаки на маршрутизацію	VPN, захищені шлюзи
Мережеві функції (NF)	Шкідливе ПЗ, несанкціонований доступ	Регулярний аудит, оновлення систем
Контроль доступу	Атаки грубої сили, компрометація облікових записів	Системи виявлення вторгнень (IDS), контроль доступу
Інфраструктура хмарних обчислень	Атаки на рівні хмарних сервісів, витоки даних	Резервування даних, хмарна ізоляція

Аутентифікація користувачів і пристроїв є ще одним важливим компонентом системи безпеки мережі 5G. Цей процес передбачає перевірку ідентичності

користувачів і пристроїв, які намагаються отримати доступ до мережі, таким чином запобігаючи проникненню несанкціонованих осіб. У контексті 5G механізми автентифікації були розроблені як надійні та ефективні, що враховують величезну кількість пристроїв, які, як очікується, підключаються до мережі [2]. Подвійний підхід автентифікації користувача з мережі та мережевої автентифікації користувача підвищує загальну безпеку, гарантуючи, що лише законні користувачі та пристрої можуть взаємодіяти з мережевими ресурсами. Ця двонаправлена модель автентифікації життєво важлива для підтримки довіри та безпеки в цифровій екосистемі, яка все більше взаємопов'язана.

Моніторинг мережевого трафіку є незамінним методом для забезпечення безпеки мереж 5G. Безперервне спостереження за потоком даних дозволяє виявляти аномалії та потенційні загрози в режимі реального часу, дозволяючи швидко втручатися до того, як станеться будь-яка значна шкода. Інструменти моніторингу мережі розроблені для аналізу величезних обсягів даних, виявлення шаблонів, які можуть вказувати на зловмисну діяльність [3]. Використовуючи передову аналітику та технології машинного навчання, ці інструменти можуть розрізняти звичайну та підозрілу поведінку, надаючи мережевим адміністраторам практичну інформацію. Цей проактивний підхід до моніторингу трафіку не тільки захищає мережу від зовнішніх загроз, але й допомагає оптимізувати продуктивність і розподіл ресурсів.

Захист Інтернету речей (IoT)

Використання безпечних протоколів зв'язку є фундаментальною стратегією захисту Інтернету речей (IoT) у контексті мереж 5G. Ці протоколи гарантують, що дані, що передаються між пристроями IoT, зашифровані та захищені від несанкціонованого доступу. Включаючи стандартизовані криптографічні алгоритми, безпечні протоколи зв'язку можуть запобігти перехопленню та фальсифікації даних, що має вирішальне значення, враховуючи величезну кількість конфіденційної інформації, яку обробляють пристрої IoT [4]. Використання захищених протоколів також полегшує автентифікацію пристрою, гарантуючи, що лише перевірені пристрої можуть спілкуватися в мережі. Цей тип надійних заходів

безпеки є незамінним для підтримки цілісності та конфіденційності даних, що передаються через екосистеми IoT з підтримкою 5G.

Сегментація мережі є ще одним ключовим заходом для підвищення безпеки IoT, особливо в розгалуженій інфраструктурі мереж 5G. Розділивши мережу IoT на менші ізольовані сегменти, організації можуть обмежити потенційне поширення кіберзагроз. Кожен сегмент можна окремо керувати та контролювати, зменшуючи ризик того, що одна вразливість зашкодить усій мережі. Сегментація також дозволяє створювати індивідуальні політики безпеки та елементи керування, що відповідають потребам кожного сегмента, таким чином оптимізуючи загальну безпеку. Впровадження сегментації в мережах IoT допомагає стримувати порушення та пом'якшувати їхній вплив, що є життєво важливим для захисту конфіденційних даних і підтримки безперервності роботи [2].

Впровадження механізмів оновлення програмного забезпечення має вирішальне значення для захисту пристроїв IoT від нових загроз і вразливостей у мережах 5G. Регулярні оновлення гарантують, що пристрої IoT оснащені найновішими виправленнями безпеки та функціями, які можуть запобігти використанню кіберзловмисниками [2]. Автоматизовані процеси оновлення можуть оптимізувати цей аспект керування безпекою, гарантуючи, що всі пристрої в мережі залишатимуться актуальними без необхідності ручного втручання. Цей підхід не тільки підвищує безпеку пристрою, але й покращує загальну стійкість мережі IoT до потенційних порушень безпеки. Підтримка актуального програмного забезпечення є важливою практикою для зменшення ризиків у динамічному середовищі IoT із підтримкою 5G.

Безпечне управління транспортними системами

У сфері безпечних систем керування трафіком шифрування каналів передачі даних є фундаментальною опорою. Шифрування гарантує, що дані, якими обмінюються транспортні засоби та центри керування, залишаються конфіденційними та захищеними від втручання. Це особливо важливо в мережах 5G, де обсяг і швидкість передачі даних значно вищі. Використовуючи надійні протоколи шифрування, такі як Advanced Encryption Standard (AES) або еліптична

криптографія, системи керування трафіком можуть захистити конфіденційну інформацію від несанкціонованого доступу [2]. Крім того, ці методи шифрування не тільки захищають дані, але й підвищують цілісність і надійність зв'язку, що є життєво важливим для підтримки безпеки та ефективності транспортних систем.

Таблиця 3.3.

Методи забезпечення кібербезпеки на основі мобільних мереж 5G для Розумних Міст

Параметр	Характеристика
Захист мережевої інфраструктури	Використання шифрування, автентифікація, моніторинг трафіку
Захист Інтернету речей (IoT)	Захищені протоколи, сегментація мережі, оновлення ПЗ
Безпечне управління транспортними системами	Шифрування каналів, аутентифікація пристроїв, виявлення аномалій
Захист критичної інфраструктури	Системи виявлення вторгнень, резервування даних, контроль доступу
Захист від атак соціальної інженерії	Навчання персоналу, багатофакторна аутентифікація, контроль поведінки
Захист кіберфізичних систем	Захищені шлюзи, інтеграція з IoT, контроль фізичного доступу
Забезпечення конфіденційності даних	Розподілені реєстри, анонімізація даних, політики зберігання
Захист мобільних додатків для міських послуг	Оновлення та аудит безпеки, захист API, блокування шкідливого коду
Захист систем розумного громадського транспорту	Захист GPS, VPN для безпечного зв'язку, контроль диспетчерських центрів

Аутентифікація пристроїв у транспортних системах є ще одним важливим компонентом для забезпечення безпеки мобільних мереж п'ятого покоління.

Оскільки транспортні засоби стають все більш підключеними, автентифікація пристроїв для перевірки їх особи перед наданням доступу до мережі є важливою. Цей процес допомагає запобігти проникненню неавторизованих пристроїв у мережу та потенційному зриву операцій. Такі технології, як інфраструктура відкритих ключів (PKI) і цифрові сертифікати, зазвичай використовуються для того, щоб лише автентифіковані пристрої могли спілкуватися в мережі [5]. Впроваджуючи надійні механізми автентифікації, транспортні системи можуть значно знизити ризик кіберзагроз, гарантуючи, що в процесі зв'язку беруть участь лише законні та надійні пристрої.

Виявлення аномалій у трафіку є важливим заходом безпеки, який доповнює шифрування та автентифікацію в транспортних системах на основі 5G. Виявлення аномалій передбачає моніторинг мережевого трафіку на наявність нерегулярних шаблонів, які можуть вказувати на зловмисну активність або системні збої. Зі збільшенням складності та обсягу даних у мережах 5G традиційних методів на основі підпису може бути недостатньо. Передові методи, такі як алгоритми машинного навчання та статистичні моделі, використовуються для виявлення відхилень від нормальної поведінки руху [6]. Ці методи дозволяють раннє виявлення потенційних загроз, дозволяючи своєчасно втручатися та розгортати стратегії пом'якшення. Використовуючи системи виявлення аномалій, транспортні мережі можуть підвищити свою стійкість проти кібератак і забезпечити безперервність безпечних операцій.

Захист критичної інфраструктури

Впровадження систем виявлення вторгнень (IDS) як методу захисту критичної інфраструктури є важливим в епоху мобільних мереж п'ятого покоління. IDS призначені для моніторингу мережевого трафіку на наявність підозрілих дій і надання сповіщень про потенційні загрози, таким чином дозволяючи вчасно втручатися, щоб запобігти несанкціонованому доступу або витоку даних [7]. Цей проактивний підхід не тільки допомагає виявити потенційні вразливості, але й сприяє постійному вдосконаленню заходів кібербезпеки. IDS можна інтегрувати з іншими системами безпеки, щоб підвищити їх ефективність і забезпечити

комплексне рішення безпеки. Використовуючи передові алгоритми та машинне навчання, IDS може адаптуватися до нових шаблонів загроз, забезпечуючи стійкість системи до нових кіберзагроз.

Резервне копіювання та відновлення даних є важливими компонентами надійної стратегії кібербезпеки, особливо для критичної інфраструктури, яка залежить від мобільних мереж п'ятого покоління. Процес регулярного резервного копіювання даних гарантує, що у разі кібератаки дані можуть бути відновлені до початкового стану з мінімальними перебоями в роботі. Цей підхід мінімізує час простою та захищає від втрати даних, що може мати серйозні наслідки для критично важливих систем [6]. Крім того, впровадження комплексного плану відновлення даних гарантує, що інфраструктура може швидко відновлюватися після інцидентів, зберігаючи безперервність і довіру. Автоматичне резервне копіювання та безпечні рішення для зберігання ще більше зміцнюють стійкість критичної інфраструктури до потенційних загроз.

Контроль доступу до життєво важливих систем є ще однією ключовою стратегією захисту критичної інфраструктури в рамках мобільних мереж п'ятого покоління. Впровадження суворого контролю доступу гарантує, що лише авторизований персонал може отримати доступ до конфіденційних систем і даних, тим самим зменшуючи ризик несанкціонованого доступу та потенційних порушень [8]. Основні заходи включають багатофакторну автентифікацію, контроль доступу на основі ролей і регулярні аудити для забезпечення відповідності протоколам безпеки. Обмежуючи доступ до основних систем, організації можуть краще захищатися від внутрішніх і зовнішніх загроз, зберігаючи цілісність і конфіденційність критично важливих операцій. Цей багаторівневий підхід до безпеки є основоположним для підтримки безпечної інфраструктури перед обличчям складних кіберзагроз.

Захист від атак соціальної інженерії

У сфері кібербезпеки навчання персоналу та мешканців стає важливою стратегією боротьби з атаками соціальної інженерії. Визнаючи, що люди часто є найслабшою ланкою в ланцюжку безпеки, організації повинні інвестувати в

комплексні освітні програми. Ці ініціативи мають бути спрямовані на те, щоб надати персоналу та мешканцям знання про загальні тактики, які використовуються в соціальній інженерії, такі як фішинг, перетекстування та цькування. Поінформована та пильна робоча сила може суттєво зменшити ймовірність успішних атак, розпізнавши попереджувальні сигнали та застосувавши найкращі методи поведінки в Інтернеті. Розвиваючи культуру обізнаності про безпеку, організації не лише захищають власні активи, але й роблять внесок у ширшу систему національної безпеки [9].

Впровадження багатофакторної автентифікації (MFA) є ще одним важливим заходом для посилення захисту від атак соціальної інженерії. MFA вимагає від користувачів надавати кілька форм перевірки перед отриманням доступу до конфіденційної інформації, що значно знижує ризик несанкціонованого доступу. Цей метод зазвичай передбачає поєднання того, що користувач знає (наприклад, пароль), чогось у нього є (наприклад, смартфон) і чогось ним є (біометрична перевірка) [10]. Включивши MFA у свої протоколи безпеки, організації значно ускладнюють зловмисникам скомпрометувати облікові записи, навіть якщо їм вдається отримати пароль користувача обманним шляхом. Цей багаторівневий підхід до безпеки може ефективно запобігти багатьом спробам соціальної інженерії та захистити важливі дані.

Моніторинг поведінки користувачів на наявність аномалій є ще однією ключовою стратегією боротьби із загрозами соціальної інженерії. Впроваджуючи системи, які спостерігають і аналізують діяльність користувачів, організації можуть ідентифікувати шаблони, які відхиляються від норми, що може вказувати на порушення або спробу атаки. Цей метод ґрунтується на розумінні типової поведінки користувачів у мережі та встановленні контрольних показників для нормальної активності [11]. Коли виявляються аномалії, такі як незвичайний час входу або доступ до нетипових файлів, служби безпеки можуть швидко дослідити та відреагувати. Цей проактивний підхід не тільки допомагає завчасно виявляти потенційні загрози, але й зміцнює загальну безпеку, запобігаючи несанкціонованому доступу до конфіденційних систем.

Захист кіберфізичних систем

Використання захищених шлюзів є фундаментальним підходом до захисту кіберфізичних систем, особливо в контексті мобільних мереж п'ятого покоління. Ці шлюзи діють як бар'єри, які запобігають несанкціонованому доступу, зберігаючи при цьому цілісність і конфіденційність даних, що передаються. Впроваджуючи захищені шлюзи, організації можуть гарантувати, що лише автентифіковані користувачі та пристрої зможуть отримати доступ до мережі, тим самим зменшуючи ризик витоку даних і кібератак. Цей підхід узгоджується з ширшою концепцією безпеки мережі в 5G, яка наголошує на автентифікації користувача та мережі [2]. Крім того, захищені шлюзи полегшують моніторинг потоку даних, уможливлюючи раннє виявлення будь-яких підозрілих дій, пропонуючи таким чином додатковий рівень безпеки.

Інтеграція систем безпеки з Інтернетом речей (IoT) має ключове значення для захисту кіберфізичних систем. Взаємозв'язок різних пристроїв через IoT представляє унікальні виклики безпеці, оскільки кожен підключений пристрій потенційно може стати точкою вразливості. Щоб вирішити цю проблему, організації повинні прийняти комплексні заходи безпеки, які включають автентифікацію пристрою, шифрування та регулярні оновлення безпеки. Ці методи гарантують, що навіть якщо один пристрій скомпрометовано, це не призведе до ширшого порушення мережі. Інтеграція систем безпеки з IoT не тільки покращує захист даних, але й оптимізує управління та контроль цих пристроїв, таким чином посилюючи стійкість мережі проти кіберзагроз [2].

Контроль фізичного доступу є ще одним важливим компонентом безпеки кіберфізичної системи. У середовищі з підтримкою 5G, де дані та операції сильно взаємопов'язані, неавторизований фізичний доступ може призвести до значних уразливостей. Впровадження суворих заходів контролю доступу, таких як біометрична автентифікація та системи спостереження, може ефективно зменшити ці ризики. Ці заходи гарантують, що тільки уповноважений персонал може отримати доступ до чутливих зон, тим самим запобігаючи несанкціонованим змінам або порушенням роботи системи. Крім того, інтеграція засобів контролю

фізичного доступу з цифровими протоколами безпеки створює цілісну структуру безпеки, яка є важливою для захисту критичної інфраструктури в епоху цифрових технологій [12].

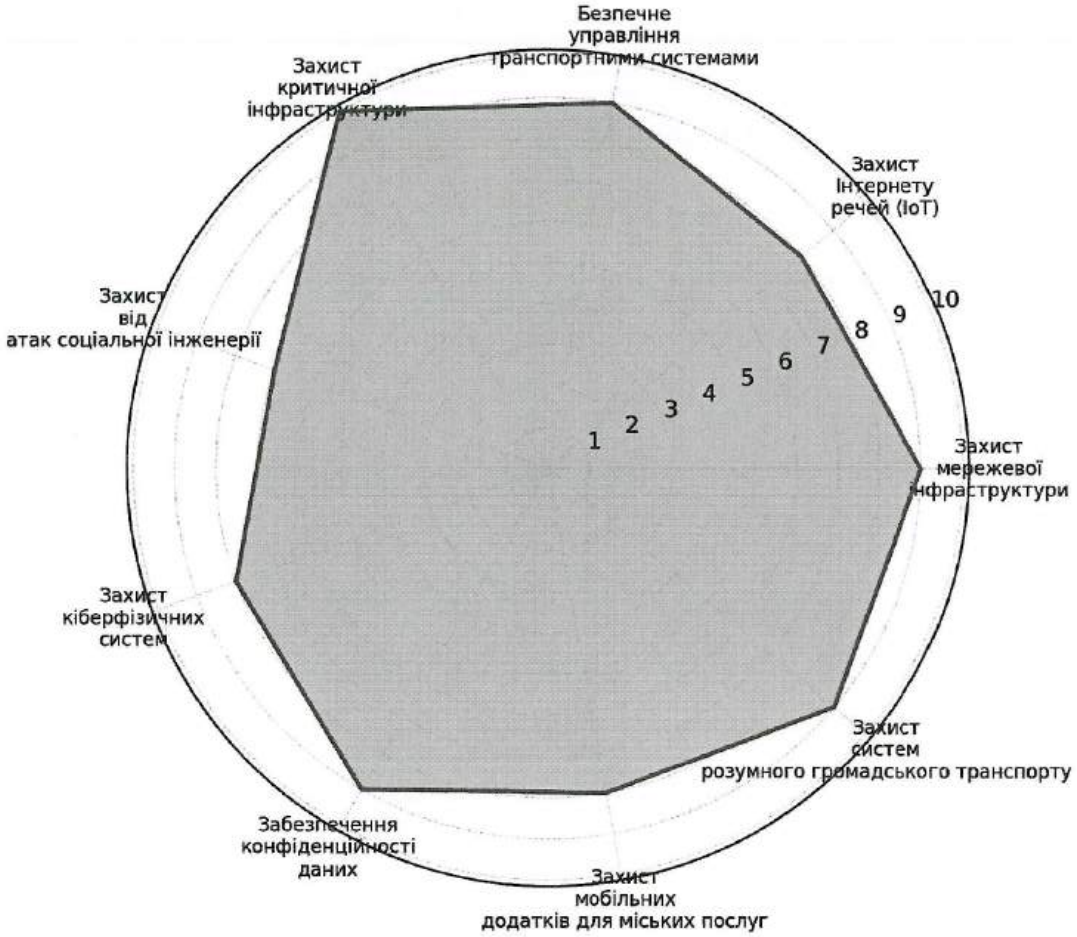


Рис. 3.1. Вплив параметрів забезпечення кібербезпеки

ВИСНОВКИ

У першому розділі досліджено ключові компоненти телекомунікаційної інфраструктури розумного міста. Підрозділ 1.1 присвячений аналізу основних елементів інфраструктури, таких як інтелектуальне управління транспортом, автономні транспортні засоби, розумні мережі енергопостачання та інші важливі складові. Представлена таблиця 1.1 систематизує ці компоненти, висвітлюючи їхні функції та значення для міського середовища. Особливу увагу приділено використанню технологій IoT та аналітики великих даних, які сприяють ефективному керуванню транспортними потоками та енергоресурсами.

У підрозділі 1.2 розглянуто архітектуру телекомунікаційної інфраструктури, необхідну для підтримки функціонування розумного міста. В таблиці 1.2 наведено вимоги до інфраструктури, такі як продуктивність, надійність, безпека та масштабованість. Також підкреслено значення сучасних технологій, зокрема 5G та Wi-Fi 6, для забезпечення швидкого та надійного з'єднання між компонентами міської інфраструктури. Представлені рисунки ілюструють архітектуру мережевих рішень, відображаючи взаємодію різних елементів у рамках концепції Smart City.

У другому розділі досліджено архітектурні особливості мобільних мереж 5G та їхню роль у розвитку інфраструктури розумного міста. Основну увагу приділено ключовим технологіям, таким як нарізка мережі (Network Slicing), масивний MIMO (Massive MIMO), формування променя (Beamforming), малі комірки (Small Cells) та граничні обчислення (Edge Computing). Аналіз рисунків і таблиць показує, що ці технології сприяють оптимальному розподілу мережевих ресурсів, підвищенню пропускної здатності, зниженню затримок та забезпеченню високої надійності з'єднань. Зокрема, рисунки ілюструють концептуальну реалізацію таких технологій, як Beamforming та Massive MIMO, що підкреслює їхню важливість у підвищенні ефективності передачі даних та зменшенні інтерференції. Таблиця 2.1 систематизує переваги архітектурних рішень, що дозволяє оцінити їхній вплив на продуктивність мережі та відповідність вимогам розумного міста.

Систематизовано переваги використання мобільних мереж 5G у розумному місті, зокрема покращення якості зв'язку, впровадження Інтернету речей (IoT), оптимізацію транспортних систем, енергетичних мереж і систем безпеки. Аналіз рисунків та таблиць свідчить, що технологія 5G забезпечує значне зниження затримок, підвищену пропускну здатність та підтримку великої кількості підключених пристроїв, що є критично важливим для функціонування розумного міста. Представлений рисунок демонструє переваги впровадження 5G у різних секторах міської інфраструктури, таких як транспорт, енергетика та безпека, тоді як таблиця 2.2 порівнює основні параметри мереж 4G та 5G, підтверджуючи суттєві покращення в швидкості, енергоефективності та надійності зв'язку.

У третьому розділі розроблено методи забезпечення кібербезпеки в інфраструктурі розумного міста з використанням технології 5G. У підрозділі 3.1 проаналізовано потенційні загрози та вразливості мережевої інфраструктури розумного міста, що базується на 5G. Проведено аналіз ключових загроз, таких як атаки на базові станції, перехоплення трафіку та вразливості мережевих протоколів. На основі результатів аналізу, представлених у таблиці 3.1, запропоновано заходи безпеки, серед яких використання шифрування, багаторівневої автентифікації та постійного моніторингу трафіку.

У підрозділі 3.2 запропоновано методи підвищення рівня захисту мережевої інфраструктури 5G у розумному місті. Представлені заходи безпеки охоплюють різні аспекти інфраструктури, включаючи захист Інтернету речей (IoT), безпечне управління транспортними системами, захист мобільних додатків та забезпечення конфіденційності даних. Таблиця 3.2 узагальнює основні методи безпеки, такі як використання захищених протоколів зв'язку, сегментація мережі, резервне копіювання даних та багаторівнева система аутентифікації. Рисунок 3.1 показує вплив впровадження запропонованих методів на зменшення кіберризиків, підвищення надійності та стійкості інфраструктури.

Таким чином, розроблені в третьому розділі методи кібербезпеки враховують особливості технології 5G і можуть бути використані для захисту критичної інфраструктури розумного міста від сучасних загроз та атак.

ПЕРЕЛІК ПОСИЛАНЬ

1. Yang C., Liang P., Fu L., Cui G., Huang F., Teng F., Bangash Y. A. Using 5G in Smart Cities: A Systematic Mapping Study // *arXiv preprint arXiv:2202.04312*. 2022.

2. Han H., Zhai W., Zhao J. Smart City Enabled by 5G/6G Networks: An Intelligent Hybrid Random Access Scheme // *arXiv preprint arXiv:2101.06421*. 2021.

3. Rito P., Almeida A., Figueiredo A., Gomes C., Teixeira P., Rosmaninho R., Oliveira A. Aveiro Tech City Living Lab: A Communication, Sensing and Computing Platform for City Environments // *arXiv preprint arXiv:2207.12200*. 2022.

4. Han T., Ge X., Wang L., Kwak K. S., Han Y., Liu X. 5G Converged Cell-less Communications in Smart Cities // *arXiv preprint arXiv:1609.06632*. 2016.

5. Khan L. U., Yaqoob I., Tran N. H., Kazmi S. M. A., Dang T. N., Hong C. S. Edge Computing Enabled Smart Cities: A Comprehensive Survey // *IEEE Internet of Things Journal*. 2022. Vol. 9, No. 1. P. 485–505. DOI: 10.1109/JIOT.2021.3063681.

6. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for Smart Cities // *IEEE Internet of Things Journal*. 2014. Vol. 1, No. 1. P. 22–32. DOI: 10.1109/JIOT.2014.2306328.

7. Taleb T., Samdanis K., Mada B., Flinck H., Dutta S., Sabella D. On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture & Orchestration // *IEEE Communications Surveys & Tutorials*. 2017. Vol. 19, No. 3. P. 1657–1681. DOI: 10.1109/COMST.2017.2705720.

8. Li Y., Chen M., Hu L., Wang Z., Zhang W. Software-Defined Network Function Virtualization: A Survey // *IEEE Access*. 2015. Vol. 3. P. 2542–2553. DOI: 10.1109/ACCESS.2015.2499271.

9. Bonomi F., Milito R., Zhu J., Addepalli S. Fog Computing and Its Role in the Internet of Things // *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing*. 2012. P. 13–16. DOI: 10.1145/2342509.2342513

10. Hu F., Hao Q., Bao K. A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation // *IEEE Communications Surveys & Tutorials*. 2014. Vol. 16, No. 4. P. 2181–2206. DOI: 10.1109/COMST.2014.2326417.

11. Zhang H., Liu N., Chu X., Long K., Aghvami A. H., Leung V. C. M. Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges // *IEEE Communications Magazine*. 2017. Vol. 55, No. 8. P. 138–145. DOI: 10.1109/MCOM.2017.1600940.

12. Wang C.-X., Haider F., Gao X., You X.-H., Yang Y., Yuan D., Aggoune H. M., Haas H., Fletcher S., Hepsaydir E. Cellular Architecture and Key Technologies for 5G Wireless Communication Networks // *IEEE Communications Magazine*. 2014. Vol. 52, No. 2. P. 122–130. DOI: 10.1109/MCOM.2014.6736752.

13. Shafi M., Molisch A. F., Smith P. J., Haustein T., Zhu P., De Silva P., Tufvesson F., Benjebbour A., Wunder G. 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice // *IEEE Journal on Selected Areas in Communications*. 2017. Vol. 35, No. 6. P. 1201–1221. DOI: 10.1109/JSAC.2017.2692307.

14. Akyildiz I. F., Nie S., Lin S.-C., Chandrasekaran M. 5G Roadmap: 10 Key Enabling Technologies // *Computer Networks*. 2016. Vol. 106. P. 17–48. DOI: 10.1016/j.comnet.2016.06.010.

15. Osseiran A., Boccardi F., Braun V., Kusume K., Marsch P., Maternia M., Queseth O., Schellmann M., Schotten H., Taoka H., Tullberg H., Uusitalo M. A., Timus B., Fallgren M. Scenarios for 5G Mobile and Wireless Communications: The Vision of the METIS Project // *IEEE Communications Magazine*. 2014. Vol. 52, No. 5. P. 26–35. DOI: 10.1109/MCOM.2014.6815890.

16. Kim K., Alshenaifi I. M., Ramachandran S., Kim J., Zia T., Almorjan A. Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive Literature Review and Survey // *Sensors*. 2023. Vol. 23, No. 7. P. 3681. DOI: 10.3390/s23073681.

17. Pirbhulal S., Chockalingam S., Shukla A., Abie H. IoT Cybersecurity in 5G and Beyond: A Systematic Literature Review // *International Journal of Information Security*. 2024. Vol. 23. P. 2827–2879. DOI: 10.1007/s10207-024-00865-5.

18. Khan R. A., Khan M. W. Cyber Security's Influence on Smart Cities: Challenges and Solutions // *AIP Conference Proceedings*. 2023. Vol. 2821, No. 1. P. 040033. DOI: 10.1063/5.0159218.

19. Wright M., Chizari H., Viana T. A Systematic Review of Smart City Infrastructure Threat Modelling Methodologies: A Bayesian Focused Review // *Sustainability*. 2022. Vol. 14, No. 16. P. 10368. DOI: 10.3390/su141610368.

20. Cui L., Xie G., Qu Y., Gao L., Yang Y. Security and Privacy in Smart Cities: Challenges and Opportunities // *IEEE Access*. 2018. Vol. 6. P. 46134–46145. DOI: 10.1109/ACCESS.2018.2853985.

21. Alamer M., Almaiah M. A. Cybersecurity in Smart City: A Systematic Mapping Study // *IEEE*. 2021. P. 719–723.

22. Mohamed N., Al-Jaroodi J., Jawhar I. Opportunities and Challenges of Data-Driven Cybersecurity for Smart Cities // *IEEE Systems Security Symposium (SSS)*. 2020. P. 1–7.

23. Khatoun R., Zeadally S. Cybersecurity and Privacy Solutions in Smart Cities // *IEEE Communications Magazine*. 2017. Vol. 55, No. 3. P. 51–59. DOI: 10.1109/MCOM.2017.1600297CM.

24. Lee J., Kim J., Seo J. Cyber Attack Scenarios on Smart City and Their Ripple Effects // *International Conference on Platform Technology and Service (PlatCon)*. 2019. P. 1–5.

25. Aldairi A., Tawalbeh L. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies // *Procedia Computer Science*. 2017. Vol. 109. P. 1086–1091. DOI: 10.1016/j.procs.2017.05.391.

26. Osseiran A., Boccardi F., Braun V., Kusume K., Marsch P., Maternia M., Queseth O., Schellmann M., Schotten H., Taoka H., Tullberg H., Uusitalo M. A., Timus B., Fallgren M. Scenarios for 5G Mobile and Wireless Communications: The Vision of the METIS Project // *IEEE Communications Magazine*. 2014. Vol. 52, No. 5. P. 26–35. DOI: 10.1109/MCOM.2014.6815890.

27. Shafi M., Molisch A. F., Smith P. J., Haustein T., Zhu P., De Silva P., Tufvesson F., Benjebbour A., Wunder G. 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice // *IEEE Journal on Selected Areas in Communications*. 2017. Vol. 35, No. 6. P. 1201–1221. DOI: 10.1109/JSAC.2017.2692307.

28. Akyildiz I. F., Nie S., Lin S.-C., Chandrasekaran M. 5G Roadmap: 10 Key Enabling Technologies // *Computer Networks*. 2016. Vol. 106. P. 17–48. DOI: 10.1016/j.comnet.2016.06.010.

29. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for Smart Cities // *IEEE Internet of Things Journal*. 2014. Vol. 1, No. 1. P. 22–32. DOI: 10.1109/JIOT.2014.2306328.

30. Taleb T., Samdanis K., Mada B., Flinck H., Dutta S., Sabella D. On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture & Orchestration // *IEEE Communications Surveys & Tutorials*. 2017. Vol. 19, No. 3. P. 1657–1681. DOI: 10.1109/COMST.2017.2705720.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ



Презентація по магістерській роботі
на тему:

Метод забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління

Виконав: Сергій ЛИСЕНКО

Керівник: Любов БЕРКМАН, д.т.н., професор

Мета роботи

Мета роботи – дослідження методів забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління.

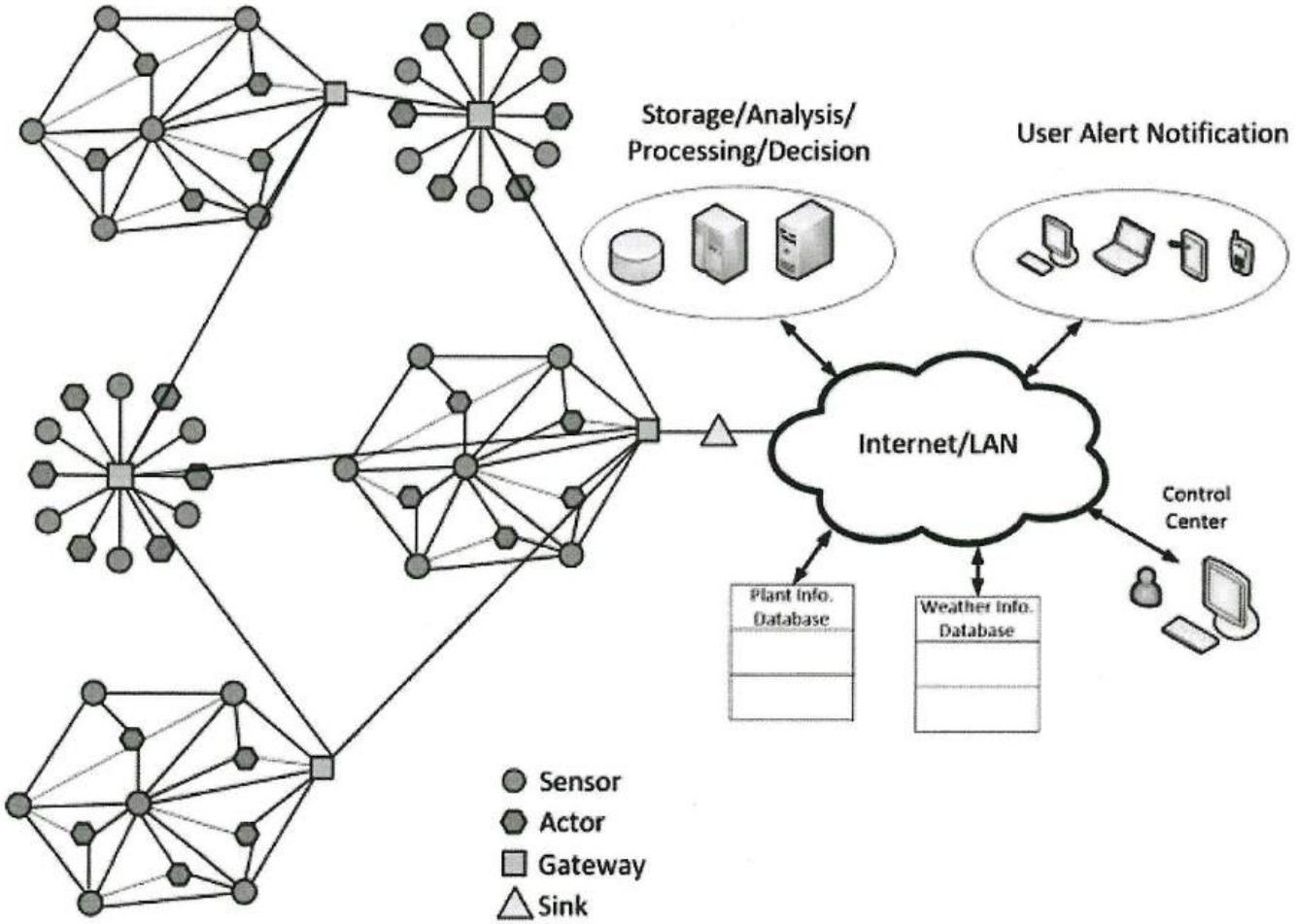
Об'єкт дослідження – процес взаємодії Розумного Міста і мереж п'ятого покоління.

Предмет дослідження – методи забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління.

Телекомунікаційна архітектура для побудови Розумного Міста

	Компонент	Призначення	Переваги
1	Мережі передачі даних	Забезпечення ефективної передачі даних у смарт-місті	Швидке та надійне підключення між системами
2	Системи зберігання інформації	Обробка та зберігання великих обсягів міських даних	Безпека та масштабованість
3	Корпоративні мережі	Інтеграція користувачів і термінальних пристроїв	Гнучкість інтеграції з іншими системами
4	Мережеві технології (5G, Wi-Fi 6)	Підтримка безперебійного зв'язку	Висока пропускна здатність і низька затримка
5	Волоконно-оптичні мережі	Високошвидкісний зв'язок для критичних додатків	Надійність та енергоефективність
6	Супутниковий зв'язок	Забезпечення зв'язку у віддалених районах	Глобальне покриття та резервування зв'язку
7	IoT-пристрої та сенсори	Збір даних у реальному часі для міських систем	Оперативний моніторинг міської інфраструктури
8	Хмарні обчислення	Обробка даних на вимогу та масштабування	Гнучкість, економія ресурсів
9	Системи безпеки та управління доступом	Захист телекомунікацій ної інфраструктури	Підвищення рівня кібербезпеки

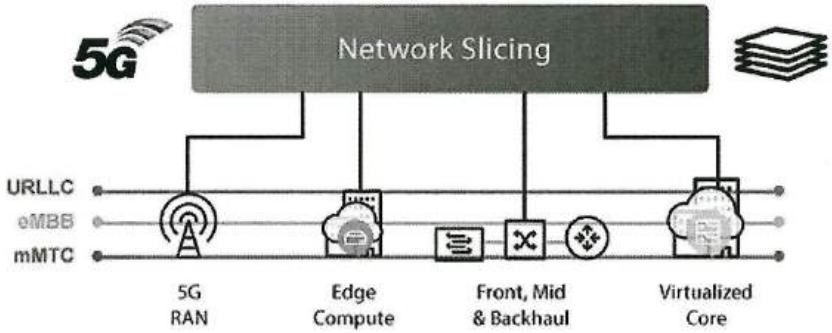
Телекомунікаційна архітектура для побудови Розумного Міста

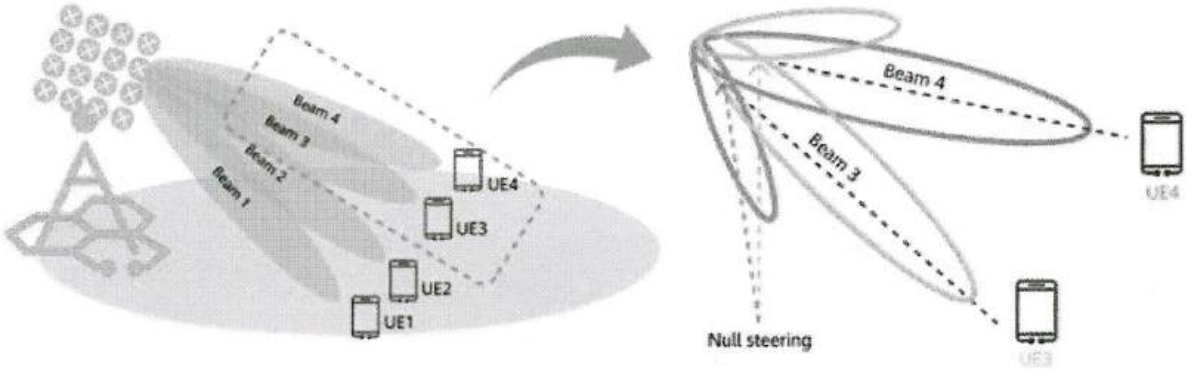


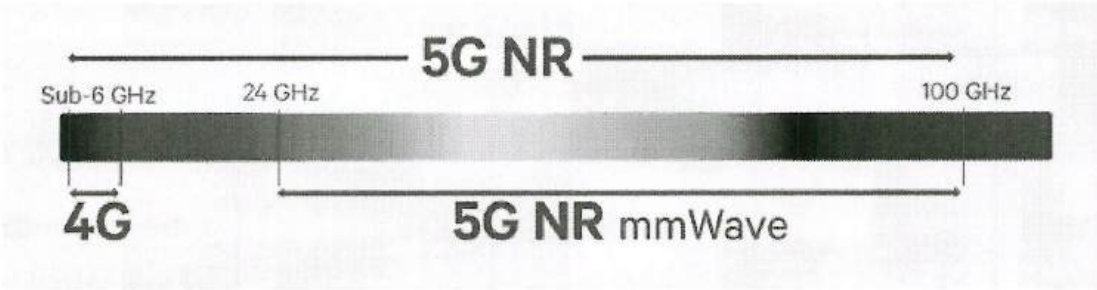
Архітектурні особливості мобільних мереж 5G

Архітектурна особливість	Призначення	Переваги
Нарізка мережі (Network Slicing)	Дозволяє створювати кілька логічних мереж в одній фізичній інфраструктурі	Гнучкість, оптимізація ресурсів, адаптація під різні потреби
Масивний MIMO (Massive MIMO)	Збільшує пропускну здатність та покращує ефективність спектру	Збільшення кількості підключених пристроїв, підвищення продуктивності
Формування променя (Beamforming)	Спрямовує сигнал на конкретного користувача для покращення зв'язку	Зниження інтерференції, покращення пропускної здатності
Малі комірки (Small Cells)	Забезпечують розширене покриття та підвищену ємність	Покращення покриття, зменшення затримок
Граничні обчислення (Edge Computing)	Обробка даних ближче до джерела для зниження затримки	Швидка обробка даних, зниження навантаження на ядро мережі
Віртуалізація мережевих функцій (NFV)	Віртуалізація мережевих функцій для підвищення гнучкості	Швидке масштабування послуг, зниження витрат на інфраструктуру
Програмно-визначена мережа (SDN)	Централізоване управління мережею для оптимізації ресурсів	Гнучке управління мережею, ефективність розподілу трафіку
Технологія міліметрових хвиль (mmWave)	Використання високочастотного спектру для підвищення швидкості	Висока швидкість передачі, підтримка нових сервісів
Покращення безпеки	Забезпечення надійного захисту даних та інфраструктури	Захист конфіденційності даних, зменшення кіберзагроз

Архітектурні особливості мобільних мереж 5G







Переваги використання 5G в Розумному Місті



Порівняння технологій 4G та 5G

Параметр	4G	5G
Максимальна швидкість передачі даних	До 1 Гбіт/с	До 10 Гбіт/с
Затримка (Latency)	20-50 мс	1-5 мс
Пропускна здатність	Нижча	Вища
Щільність підключень	100 000 пристроїв на км²	Мільйон пристроїв на км²
Ефективність спектру	Менш ефективний	Вища ефективність
Архітектура мережі	Монолітна	Модульна, з підтримкою SDN/NFV
Частотний діапазон	1-6 ГГц	До 100 ГГц (мм-хвилі)
Енергоспоживання	Високе	Знижене
Підтримка IoT	Обмежена	Повна підтримка
Безпека	Базові механізми шифрування	Розширені механізми безпеки

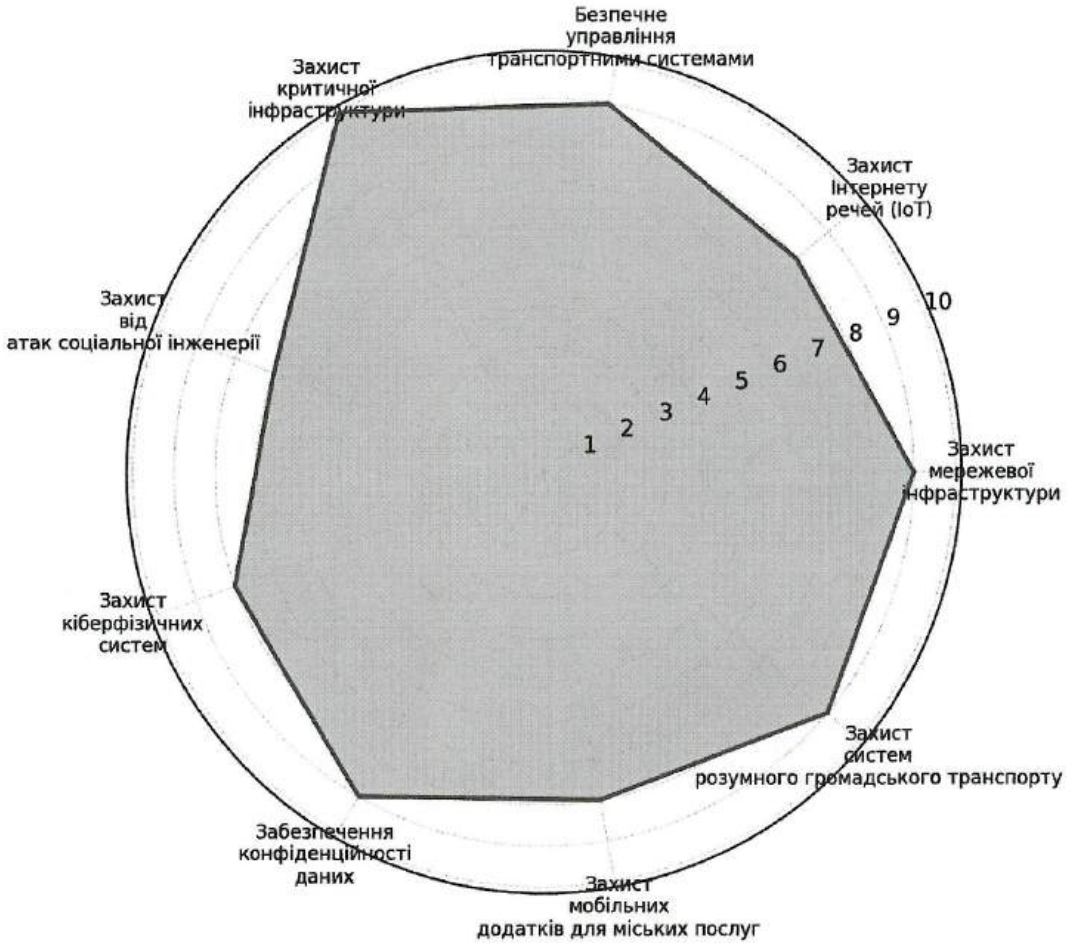
Аналіз загроз та вразливостей в інфраструктурі Розумного Міста на основі 5G

Параметр	Основні загрози	Заходи безпеки
Загрози мережевої інфраструктури	Атаки на базові станції, перехоплення трафіку, вразливість протоколів	Шифрування, аутентифікація, моніторинг
Кіберзагрози Інтернету речей (IoT)	DDoS-атаки, недостатність автентифікації, неконтрольований доступ	Захищені протоколи, багаторівнева аутентифікація, контроль доступу
Уразливості систем управління трафіком	Маніпуляція даними, підміна маршрутів, перехоплення інформації	Шифрування, захищені маршрутизаційні алгоритми, аналіз аномалій
Ризики для критичної інфраструктури	Атаки на енергомережі, вразливість водопостачання, саботаж систем	Резервування, моніторинг, багаторівнева система захисту
Вплив соціальної інженерії	Фішинг, маніпулювання даними, злом облікових записів	Навчання персоналу, багатофакторна аутентифікація, моніторинг доступу
Уразливості кіберфізичних систем	Злам систем безпеки, втручання в датчики, збої автоматизованих систем	Інтеграція безпеки IoT, захищені шлюзи, аудит безпеки
Загрози конфіденційності даних	Несанкціонований збір даних, витік через ненадійні канали, використання великих даних	Політики захисту, шифрування, контроль доступу
Вразливості мобільних додатків	Ін'єкційні атаки, незахищені API, підробка транзакцій	Регулярні оновлення, аудит, захист API
Вплив атак на громадський транспорт	Спуфінг, несанкціоноване управління, маніпуляція тарифами	Верифікація сигналів, контроль доступу, шифрування даних

Методи забезпечення кібербезпеки на основі мобільних мереж 5G для Розумних Міст

Параметр	Характеристика
Захист мережевої інфраструктури	Використання шифрування, автентифікація, моніторинг трафіку
Захист Інтернету речей (IoT)	Захищені протоколи, сегментація мережі, оновлення ПЗ
Безпечне управління транспортними системами	Шифрування каналів, аутентифікація пристроїв, виявлення аномалій
Захист критичної інфраструктури	Системи виявлення вторгнень, резервування даних, контроль доступу
Захист від атак соціальної інженерії	Навчання персоналу, багатофакторна аутентифікація, контроль поведінки
Захист кіберфізичних систем	Захищені шлюзи, інтеграція з IoT, контроль фізичного доступу
Забезпечення конфіденційності даних	Розподілені реєстри, анонімізація даних, політики зберігання
Захист мобільних додатків для міських послуг	Оновлення та аудит безпеки, захист API, блокування шкідливого коду
Захист систем розумного громадського транспорту	Захист GPS, VPN для безпечного зв'язку, контроль диспетчерських центрів

Вплив параметрів забезпечення кібербезпеки



Висновки

В магістерській роботі досягнуто наступних результатів:

У першому розділі досліджено ключові компоненти та архітектуру телекомунікаційної інфраструктури розумного міста. Проаналізовано основні елементи, такі як інтелектуальне управління транспортом, розумні енергомережі та використання технологій IoT і великих даних. Наведено вимоги до інфраструктури, включаючи продуктивність, надійність і масштабованість, а також підкреслено роль технологій 5G і Wi-Fi 6.

Другий розділ присвячено архітектурним особливостям мобільних мереж 5G у розумному місті. Розглянуто ключові технології, зокрема нарізку мережі, Massive MIMO, Beamforming і Edge Computing. Визначено їхню роль в оптимізації ресурсів, підвищенні пропускної здатності та зниженні затримок. Порівняно характеристики мереж 4G та 5G, підтверджуючи переваги останньої для міської інфраструктури.

У третьому розділі розглянуто методи забезпечення кібербезпеки інфраструктури розумного міста на основі 5G. Проаналізовано основні загрози та запропоновано заходи захисту, такі як шифрування, багаторівнева автентифікація та моніторинг трафіку. Запропоновані методи охоплюють захист IoT, транспортних систем і конфіденційності даних, забезпечуючи надійність та стійкість міської інфраструктури.

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Сергій ЛИСЕНКО

Назва: Метод забезпечення кібербезпеки в інфраструктурі Розумного Міста з використанням мобільних мереж п'ятого покоління

Координатор: Любов БЕРКМАН

Підрозділ: ННІТ

Коефіцієнт подібності 1:0.1

Коефіцієнт подібності 2:0

Тривога: 0

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

Дата *Підпис Наукового керівника*