Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження захищених мережевих архітектур та протоколів Інтернету речей у "розумних містах"

Виконав: студент VI курсу, групи СНнм-61
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)

_____ Коваль М.О.
(підпис) (прізвище та ініціали)

Керівник _____ Пасічник В.В.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Дуда О.М.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Михалик Д.М.
(підпис) (прізвище та ініціали)

Тернопіль
2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«29» травня 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Коваль Максим Олексійович
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження захищених мережевих архітектур та протоколів Інтернету речей у "розумних містах"

Керівник роботи Пасічник Володимир Володимирович., професор кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 24 » листопада 2023 року № 4/7-1100

2. Термін подання студентом завершеної роботи 27 травня 2024р.

3. Вихідні дані до роботи Наукові публікації про мережеві архітектури та протоколи Інтернету речей у "розумних містах", проблеми безпеки та захисту.

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ. 1 Аналіз предметної області. 1.1 Архітектура системи Інтернету речей. 1.2 Технології IoT. 1.3 Елементи безпеки IoT. 1.4 Розумні міста: безпека мережевого рівня. 1.5 Соціально-технічна безпеки в розумних містах. 1.6 Висновок до першого розділу. 2 Методологія захисту архітектури «розумних міст». 2.1 Виклики безпеки та конфіденційності в архітектурах IoT. 2.2 Висновок до другого розділу. 3 Безпечні архітектури «розумного міста». 3.1 Архітектури «розумних міст». 3.1.1 IoT-A. 3.1.2 iCore. 3.1.3 BUTLER. 3.1.4 OpenIoT. 3.1.5 SMARTIE 3.1.6 COSMOS. 3.1.7 COMPOSE. 3.1.8 PRISMACLOUD. 3.1.9 RERUM. 3.2 Компоненти безпечної архітектури Інтернету речей для «розумного міста». 3.2.1 Чорні мережі. 3.2.2 Довірений SDN контролер. 3.2.3 Єдиний реєстр. 3.2.4 Система управління ключами. 3.3 Протоколи для застосунків «розумного міста». 3.4 Заходи безпеки IoT. 3.4.1 ZigBee. 3.4.2 Bluetooth. 3.4.3 RFID. 3.4.4 WiFi. 3.5 Висновок до третього розділу. 4 Охорона праці та безпека в надзвичайних ситуаціях. 4.1 Питання щодо охорони праці. 4.2 Питання щодо безпеки в надзвичайних ситуаціях. 4.3 Висновок до четвертого розділу. Висновки. Додатки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1 Титульна сторінка. 2 Тема, Мета, Об'єкт, Предмет дослідження. 3 Завдання дослідження. 4 Актуальність дослідження. 5 Базова трирівнева архітектура IoT. 6 Технології IoT. 7 Компоненти та базова структура «розумного міста» які можуть бути мішенню для хакерів. 8 Архітектури безпеки COMPOSE. 9 Безпечні послуги з архітектури розумного міста на основі IoT. 10 Базові компоненти безпечної архітектури Інтернету речей для розумних міст. 11 Таксономія технологій комунікації для «розумних міст». 12 Висновки. 13 Завершальний слайд

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Сенчишин В.С., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., ст. викладач		

7. Дата видачі завдання 24 листопада 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	04.12.2023	*Виконано*
2.	Підбір наукових джерел про захищені мережеві	15.12.2023-31.11.2023	*Виконано*
	Архітектури, протоколи Інтернету речей в		
	«розумних містах»		
3.	Опрацювання наукових публікацій та збір даних по	15.01.2024-25.02.2024	*Виконано*
	темі роботи		
4.	Виконання дослідження згідно мети кваліфікаційної	26.02.2024-07.04.2024	*Виконано*
	роботи		
5.	Оформлення розділу «Аналіз предметної області»	15.04.2024-18.04.2024	*Виконано*
6.	Оформлення розділу «Методологія захисту	19.04.2024-25.04.2024	*Виконано*
	архітектури «розумних міст»		
7.	Оформлення розділу «Безпечні архітектури	26.04.2024-02.05.2024	*Виконано*
	«розумного міста»		
8.	Оформлення розділу «		
8.	Виконання завдання до підрозділу «Охорона праці»	03.05.2024-07.05.2024	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	08.05.2024-10.05.2024	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	11.05.2024-14.05.2024	*Виконано*
11.	Нормоконтроль	15.05.2024-16.05.2024	*Виконано*
12.	Перевірка на плагіат	17.05.2024	*Виконано*
13.	Попередній захист кваліфікаційної роботи	21.05.2024	*Виконано*
14.	Захист кваліфікаційної роботи	30.05.2024	

Студент _____ Коваль М.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Пасічник В.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження захищених мережевих архітектур та протоколів Інтернету речей у «розумних містах» // Кваліфікаційна робота освітнього рівня «Магістр» // Коваль Максим Олексійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНнм-61 // Тернопіль, 2024 // С. 77, рис. – 7, табл. – 1, кресл. – 13, додат. – 2, бібліогр. – 68.

Ключові слова: розумне місто, інтернет речей, безпека, протоколи, конфіденційніть, мережі, моніторинг, цілісніть.

Кваліфікаційна робота присв'ячена дослідженню захищених мережевих архітектур та протоколів Інтернету речей у «розумних містах»

В першому розділі кваліфікаційної роботи розглянуто архітектуру системи Інтернету речей. Проаналізовано елементи безпеки в «розумних містах». Обґрунтовано важливість питань захисту та безпеки для протоколів IoT.

В другому розділі кваліфікаційної роботи описано виклики безпеки та конфіденційності. Досліджено методології захисту архітектури «розумного міста»

В третьому розділі кваліфікаційної роботи запропоновано компоненти безпечної архітектури IoT та протоколів в «розумному місті»

В четвертому розділі кваліфікаційної роботи розглянуто забезпечення безпечної роботи з обладнанням.

Об'єкт дослідження мережеві архітектури та протоколи Інтернету речей (IoT), що використовуються у системах «розумних міст». Предмет дослідження. методи, алгоритми та технології забезпечення захищених мережевих архітектур і протоколів для Інтернету речей у «розумних містах».

ANNOTATION

Research on protected network architectures and Internet protocols in "smart cities" // The educational level "Master" qualification work // Koval Maksym Oleksiiovych // Ternopil Ivan Pulyuy National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, SNnm-61 group // Ternopil, 2024 // P. 77, fig. - 7, tables - 1, posters - 13, annexes - 2, ref. - 68.

Key words: smart city, internet of things, security, protocols, privacy, networks, monitoring, integrity.

The qualification work is devoted to the study of secure network architectures and protocols of the Internet of Things in "smart cities"

The first chapter of the qualification work describes the architecture of the Internet of Things system. The security elements in smart cities are analysed. The importance of security and safety issues for IoT protocols is substantiated.

The second section of the qualification work describes security and privacy challenges. The methodologies for protecting the architecture of the "smart city" are investigated

The third chapter of the thesis proposes components of a secure IoT architecture and protocols in the smart city

The fourth section of the qualification work considers ensuring safe operation of equipment.

The object of study is network architectures and protocols of the Internet of Things (IoT) used in smart city systems. The subject of research is methods, algorithms and technologies for providing secure network architectures and protocols for the Internet of Things in smart cities.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IoT (англ. Internet of Things) – Інтернет речей.

IoT – Інтернет речей

WSN (англ. Wireless sensor networks) – Бездротова сенсорна мережа

RFID (англ. Radio-frequency identification) – Радіочастотна ідентифікація

DDoS (англ. Denial-of-service attack) – Атака на відмову в обслуговуванні

ARM – (англ. Architectural reference model) – архітектурної еталонної моделі

IoT-A – (англ. Internet of Things Architecture) – Архітектура Інтернету речей

ВО – Віртуальні об’єкти

РМ – Розумне місто

ФО – Фізичні об’єкти

ЗРМ – Застосунки розумного міста

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі концепція «розумних міст» набуває все більшого значення, оскільки вона спрямована на підвищення ефективності міської інфраструктури, зниження витрат та покращення якості життя громадян. Ключовою складовою таких міст є Інтернет речей (IoT), який забезпечує зв'язок і взаємодію між різними пристроями та системами. Однак з розширенням використання IoT зростає й ризик кіберзагроз та атак, що може призвести до серйозних наслідків для безпеки та конфіденційності даних.

Дослідження захищених мережевих архітектур та протоколів IoT у контексті "розумних міст" є актуальним, оскільки передбачає аналіз таких факторів: забезпечення безпеки даних, безперебійна робота інфраструктури, захист від кібератак, відповідність стандартам, підвищення довіри громадян, усе це є ключовим для успішної реалізації концепції "розумних міст", забезпечення їх безпеки, надійності та ефективності.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є підвищення рівня повноти подання інформації щодо захищених мережевих архітектур і протоколів для Інтернету речей (IoT) у «розумних містах» з метою забезпечення високого рівня безпеки, конфіденційності даних та безперебійної роботи міської інфраструктури. Для досягнення поставленої мети потрібно виконати ряд завдань, зокрема:

– Проаналізувати стан досліджень в області існуючих мережевих архітектур та протоколів IoT

– Дослідити методи захисту архітектур та протоколів.

– Проаналізувати кіберзагрози та ризики

– Виконати порівняння існуючих поширених протоколів

– Розробити заходи безпеки компонентів «розумного міста»

Об’єкт дослідження мережеві архітектури та протоколи Інтернету речей (IoT), що використовуються у системах "розумних міст". Це включає апаратне і програмне забезпечення, комунікаційні мережі, методи захисту даних, а також

інфраструктурні елементи, які забезпечують функціонування та безпеку IoT у міському середовищі.

Предмет дослідження. методи, алгоритми та технології забезпечення захищених мережевих архітектур і протоколів для Інтернету речей (IoT) у «розумних містах». Це включає дослідження механізмів автентифікації, авторизації, шифрування даних, виявлення і запобігання кіберзагрозам, а також інтеграцію цих технологій в існуючі міські інфраструктури для підвищення їх безпеки та надійності.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що отримали подальший розвиток заходи для захищених мережевих архітектур та протоколів Інтернету речей у "розумних містах".

Практичне значення одержаних результатів. Виконано аналіз захищених мережевих архітектур та протоколів Інтернету речей у "розумних містах", подано компоненти та рекомендації захисту архітектур та протоколів.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на VII Міжнародній науково-технічній конференції «Світлотехніка й електроенергетика: історія, проблеми, перспективи» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2024 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції (Див. застосунки Б).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 68 найменувань та 2 додатки. Загальний обсяг кваліфікаційної роботи складає 83 сторінки, з них 77 сторінки основного тексту, який містить 7 рисунків та 1 таблиць.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

Останнім часом Інтернет речей (IoT) привертає до себе значну увагу через численні потенційні покращення, які він може привнести в повсякденне життя людей, спрощуючи багато з їхніх повсякденних справ. Це особливо помітно в сферах «розумних» будівель, «розумної» охорони здоров'я та «розумних» міст. Особливо в сфері «розумних міст» переваги для громадян, суспільства та економіки в цілому перетворили Інтернет речей на основний тренд, і багато муніципалітетів намагаються будувати свої стратегії розвитку міст на його основі. Звичайно, найпершим кроком є створення інфраструктури Інтернету речей, що може бути досить дорогим. Потім міста повинні розробити застосунки, які працюватимуть на базі цієї інфраструктури і відповідатимуть вимогам і потребам громадян. Остання частина дуже важлива для того, щоб мотивувати громадян використовувати і впровадити технології Інтернету речей.

Основним фактором, що спонукає громадян до використання технологій Інтернету речей в цьому напрямку, є довіра і надійність Інтернету речей в цілому. Логічно припустити, що громадяни можуть скептично ставитися до цієї нової технології, особливо коли тисячі або мільйони нових малих пристроїв можуть постійно перебувати навколо них, з потенціалом безперервного моніторингу їхньої повсякденної діяльності. Ці пристрої стають не лише меншими, але й більш інтелектуальними, автономними та активними і легко інтегруються в середовище «розумного міста».

Існують різні прогнози, що мільярди пристроїв будуть підключені до Інтернету речей протягом наступних кількох років [1, 2]. Зростаюча кількість автономних підключених пристроїв, які не лише відстежують навколишнє середовище, але й можуть впливати на нього, може стати тривожним фактором для громадян з точки зору крадіжки їхньої приватної інформації, реєстрації їхньої діяльності, моніторингу їхньої присутності або навіть заподіяння шкоди їхньому життю. Для того, щоб мотивувати користувачів впроваджувати IoT і використовувати застосунки «розумного міста» у своїй повсякденній діяльності, їм повинні бути надані гарантії того, що системи IoT:

- будуть надійними з точки зору інформації, яку вони надають
- будуть обмінюватися інформацією у безпечний спосіб
- будуть захищати їхню приватну інформацію.

Щоб задовольнити вищезазначені вимоги, вся система IoT повинна бути захищеною на міжрівневому рівні, починаючи з фізичного рівня і охоплюючи всі рівні аж до застосунків. Оскільки системи IoT базуються на бездротових сенсорних мережах, різні механізми безпеки сенсорів можуть бути прийняті і в IoT [3]. Функції безпеки і збереження конфіденційності повинні бути вбудовані в роботу системи ще на етапі проектування, оскільки посмертні виправлення і поліпшення можуть лише закрити деякі вразливості, але не забезпечать повномасштабну безпеку. Таким чином, останнім часом спостерігається рух до прийняття концепції «безпеки та конфіденційності за задумом», коли хтось хоче побудувати нову систему IoT. Концепція «безпеки за задумом» описує необхідність врахування всіх можливих проблем безпеки на етапі розробки, а також розробку відповідних механізмів для запобігання та реагування на ці проблеми [4].

Хоча для прийняття концепції «безпеки за задумом» може бути достатньо набору інструментів безпеки, для прийняття концепції «конфіденційності за задумом» потрібен більш цілісний підхід, оскільки набір технологій, що підвищують конфіденційність, не може повністю захистити конфіденційність користувачів [5]. Це вимагає вбудовування концепції конфіденційності в основу багатьох системних функцій, наприклад, на борту давачів, щоб не збирати інформацію, що дозволяє ідентифікувати особу, на шлюзах, щоб приховати інформацію, що дозволяє ідентифікувати особу, перед пересиланням зашифрованих даних, на проміжному програмному забезпеченні, щоб заборонити зв'язування інформації між різними сервісами тощо.

Окрім безпеки та конфіденційності, питання довіри до Інтернету речей також привертає багато дослідницького інтересу. Надійний Інтернет визначається в [6] як Інтернет-система, яка є безпечною, надійною і стійкою до атак і збоїв. Це означає, що поняття довіри до Інтернету речей має оцінюватися за допомогою метрик:

- надійність як систем, так і даних
- безпека інфраструктури та послуг, що надаються
- здатність системи запобігати атакам і збоям та реагувати на них.

Загальна модель довіри до Інтернету речей, оскільки вона включає в себе безпеку і конфіденційність, може бути потенційно дуже корисною для просування систем Інтернету речей серед кінцевих користувачів або громадян. Розумно припустити, що система, яка сертифікована як «надійна», буде набагато привабливішою для користувача, ніж будь-яка інша система. Однак, щоб зробити систему надійною, її функціональна архітектура повинна включати в себе всі функції безпеки, конфіденційності та довіри.

В [7] висвітлюються проблеми безпеки в IoT. Автори визначають вимоги до безпеки та виклики, які часто зустрічаються в розробках IoT. У дослідженні обговорюються загрози безпеці та їх вирішення на кожному рівні IoT для створення безпечної технології. На думку авторів в [8] звичайні політики безпеки через різні протоколи зв'язку та стеки в IoT не можуть бути застосовані до системних архітектур IoT. Це пов'язано з гетерогенною структурою IoT, пристроями, нестачею ресурсів. Він пропонує потужну інфраструктуру мережевої безпеки для захисту ризиків безпеки даних. Деякі основні обмеження і проблеми безпеки IoT розглядаються в [9].У [10] автори представляють огляд атак на рівні Інтернету речей в деяких прикладах сценаріїв, а також методологію вирішення цих проблем. Вони також складають короткий перелік існуючих методів безпеки та обмежень надійності для IoT і пропонують структуру безпеки для подолання цих обмежень. Безпека проти ефективності як актуальна проблема для продуктів IoT детально розглянута в роботі [11]. Автори дійшли висновку, що в даний час не зрозуміло, який варіант слід розглядати як правильну відповідь на застосування процедур забезпечення цілісності, доступності та конфіденційності без небажаного впливу на розподілені обчислювальні ресурси та оптимізацію енергоспоживання. У роботі [12] запропонували метод для кращого визначення загроз, які можуть змінитися з новим соціально-технічним середовищем, створеним IoT. Вони рекомендують, що розробка IoT повинна включати безпеку без особливих зусиль, оскільки

практично жоден споживач не є експертом з IT-безпеки. Це повинно включати взаємодію між екосистемами пристроїв - не можна очікувати, що користувачі будуть виконувати позитивні дії, щоб компенсувати недоліки безпеки». Загрози безпеці та вразливості, пов'язані з «розумними» містами, проаналізували в роботі [13]. Вони запропонували деякі найкращі практики, засновані на трьох факторах: технологічному, соціально-економічному та управлінському. Проблеми кібербезпеки, такі як конфіденційність, безпека та захист у «розумних» містах, також обговорювали в роботі [14], де представили широкий огляд питань, пов'язаних з безпекою в рамках «розумних» міст. У статті йдеться про вразливості і загрози безпеки в інтернеті речей з метою підвищення обізнаності громадськості. Автори обговорили такі питання, як гетерогенність, повсюдність в контексті безпеки Інтернету речей. Вони вважають, що міські менеджери повинні мудро управляти поняттями ризику і безпеки, а також конфіденційності. А також влада повинна бути добре поінформована про всі питання, пов'язані з безпекою розумного міста. Ця стаття є стислим поясненням концепції безпеки в загальній архітектурі IoT і намагається дати інше бачення проблем безпеки розумних міст IoT.

1.1 Архітектура системи Інтернету речей

В основному, найпоширеніша архітектура IoT складається з трьох рівнів [14], як показано на Рисунку 1.1:

Рисунок 1.1 – Базова 3-рівнева архітектура IoT

Фізичний рівень - це рівень сприйняття, який включає в себе сенсорні пристрої. Цей рівень відповідає за збір сенсорних даних і надсилає їх до шлюзу, а потім доставляє їх до хмарної системи для подальшої обробки. Мережевий рівень забезпечує зв'язок між хмарою шлюзу розумних пристроїв і серверами, а також керує сигналізацією. Прикладний рівень - це інтерфейс користувача, який взаємодіє з іншими рівнями і надає різні послуги для користувачів.

1.2 Технології IoT

IoT використовує набір технологій, таких як Інтернет, RFID та бездротові сенсорні мережі (WSN) для забезпечення зв'язку між вузлами. WSN включає в себе сенсорні вузли, які визначають події та дії і надсилають дані на базову станцію (поглинач) для подальшого опрацювання. Пристрій радіочастотної ідентифікації (RFID) - це ще одна технологія, яка забезпечує унікальну ідентифікацію об'єктів і дозволяє їх відстежувати. На рисунках 1.2 і .1.3 показана базова структура технологій RFID і WSN.

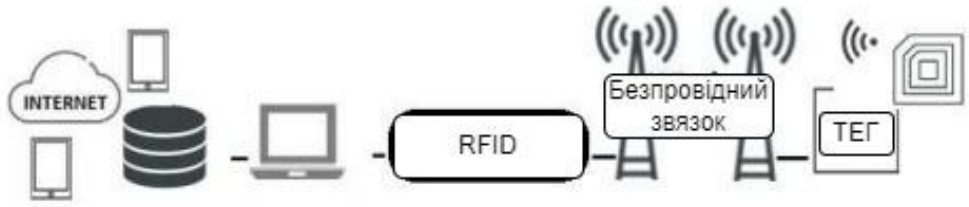

Рисунок 1.2 – Проста структура RFID-платформи

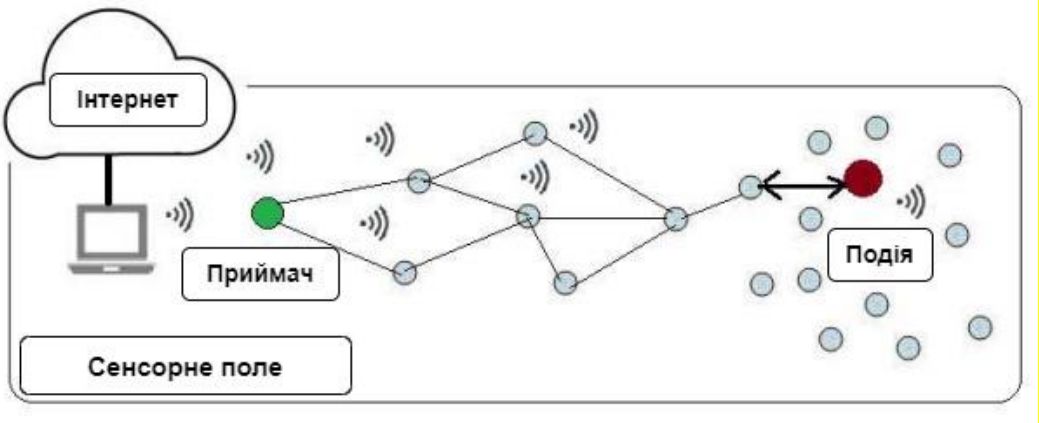

Рисунок 1.3 – Базова архітектура WSN

1.3 Елементи безпеки IoT

Виходячи з базової моделі IoT, розглянемо проблеми безпеки на кожному рівні.

1. Проблеми безпеки на рівні сприйняття

Всі традиційні проблеми безпеки в Інтернеті, на додаток до проблем безпеки, прийнятих в IoT, є проблемами безпеки на рівні сприйняття. Загрози на цьому рівні пов'язані з вузлом зондування, радіосигналами і фізичними атаками [16] Безпека вузлів і пристроїв: RFID, RSN, NFC і бездротові сенсорні пристрої - це дві основні технології, які підтримують і розвивають IoT. Всі вразливості, пов'язані з цими технологіями, автоматично перетворюються на вразливості пристроїв IoT. Ризики безпеки, такі як прослуховування вузла, підробка, атака канального рівня, втрата даних, відстеження тегів, контроль живлення, атака затоплення, збій та пошкодження апаратного вузла, атака на вузол, помилковий або забруднений шумом сенсорний сигнал.

2. Проблеми безпеки мережевого рівня

Першою проблемою на цьому рівні є «підключення». Цей рівень може діяти як проміжний між користувацьким застосунком і рівнем сприйняття. Він є дуже вразливим до атак через великий обсяг інформації, яку необхідно передати до хмарної системи. Вузьке місце або перевантаження мережі, DOS, зберігання, несанкціоновані атаки можуть бути серйозною проблемою [17]. Основні проблеми безпеки можуть включати в себе WiFi, Bluetooth та інфрачервоний зв'язок, мережу доступу 3 і 4G, безпеку ліній електропередач, сигналізацію, LAN, WAN і безпеку протоколів [18].

3. Проблеми безпеки на рівні застосунків

Те, що може статися на цьому рівні, відбувається на програмному рівні. Після успішної атаки на цьому рівні додаток може бути модифікований або закритий. Відмова в обслуговуванні є типовим наслідком проблеми безпеки. Атаки зловмисного коду, витік даних, перевантаження даних, втрата даних, аутентифікація даних, пошкодження інтерфейсу і програмного забезпечення,

потоки мобільних обчислень, збій ОС, звичайні віруси на базі Windows/OS для мобільних пристроїв перераховані як основні проблеми на рівні застосунків IoT.

1.4 Розумні міста: безпека мережевого рівня

«Розумні міста» розглядаються як соціотехнічна система. «Розумне місто» - це соціотехнічна інформаційна система, що підтримує розвиток таких технологій, як Інтернет, інформаційні та комунікаційні технології, хмарні обчислення, віртуалізація та Інтернет речей. Власне, розумні міста використовують IoT для того, щоб реалізувати свої компоненти і підвищити ефективність своїх послуг, а також заохотити своїх громадян до участі у всіх соціально-технічних заходах. З розвитком Інтернету речей все більше підключених об'єктів поширюються і використовуються у розгортанні «розумних» міст. Таким чином, з'являється більше проблем безпеки і більше потенційних кіберзагроз, з якими потрібно боротися [19].

Існує перелік вражаючих атак, які можуть бути здійснені зловмисниками на мережевому рівні, такі як Позбавлення сну, самонаведення, MITM-атака, DoS, перенаправлення, підробка підтверджень, порушення цілісності, шкідливий код, підробка, зміна інформації про маршрутизацію, порушення цілісності потоків передачі, червоточина, атаки на маршрутизацію, проблеми з протоколом, порушення мережевого з'єднання, порушення цілісності Sybil, потоп Hello, фізичні збої, вирва і порушення цілісності Internet Smurf [20].

Хоча питання безпеки «розумних міст» є багаторівневими, але найбільш складними небезпечними атаками можуть бути спроби вимкнути глобальну мережу зв'язку. Структура IoT базується на бездротових технологічних з'єднаннях, які вимагають високошвидкісного широкосмугового зв'язку з великою швидкістю передачі даних. З'єднання базується на поєднанні волоконної оптики, 3G/4G, Bluetooth, ZigBee, LTE технологій для забезпечення зв'язку з численними сервісами. Система зв'язку, яка зазвичай є комбінацією дротових і бездротових мереж [21]. Атака на систему зв'язку може призвести до повного виведення з ладу всієї системи. Це може бути здійснено кількома

зловмисниками проти бездротової телекомунікаційної інфраструктури. Такі атаки мають великий потенціал вивести з ладу мережу зв'язку, а отже, вплинути на всі мережі та послуги. Зловмисники можуть діяти як з внутрішньої, так і з зовнішньої зони.

4. Зовнішні атаки

Можливе зовнішнє вторгнення ззовні структури: Зловмисники повинні пройти кілька рівнів, щоб дістатися до службового рівня.

5. Внутрішні атаки

Зловмисний користувач (місцеві хакери) має намір відключити будь-який сервіс, намагаючись реалізувати DoS-атаку зсередини мережі.

На Рисунку 1.4 показано схему «розумного міста», що включає мережевий рівень та підрівень послуг, а також найважливіші компоненти, які можуть бути мішенню для хакерів.

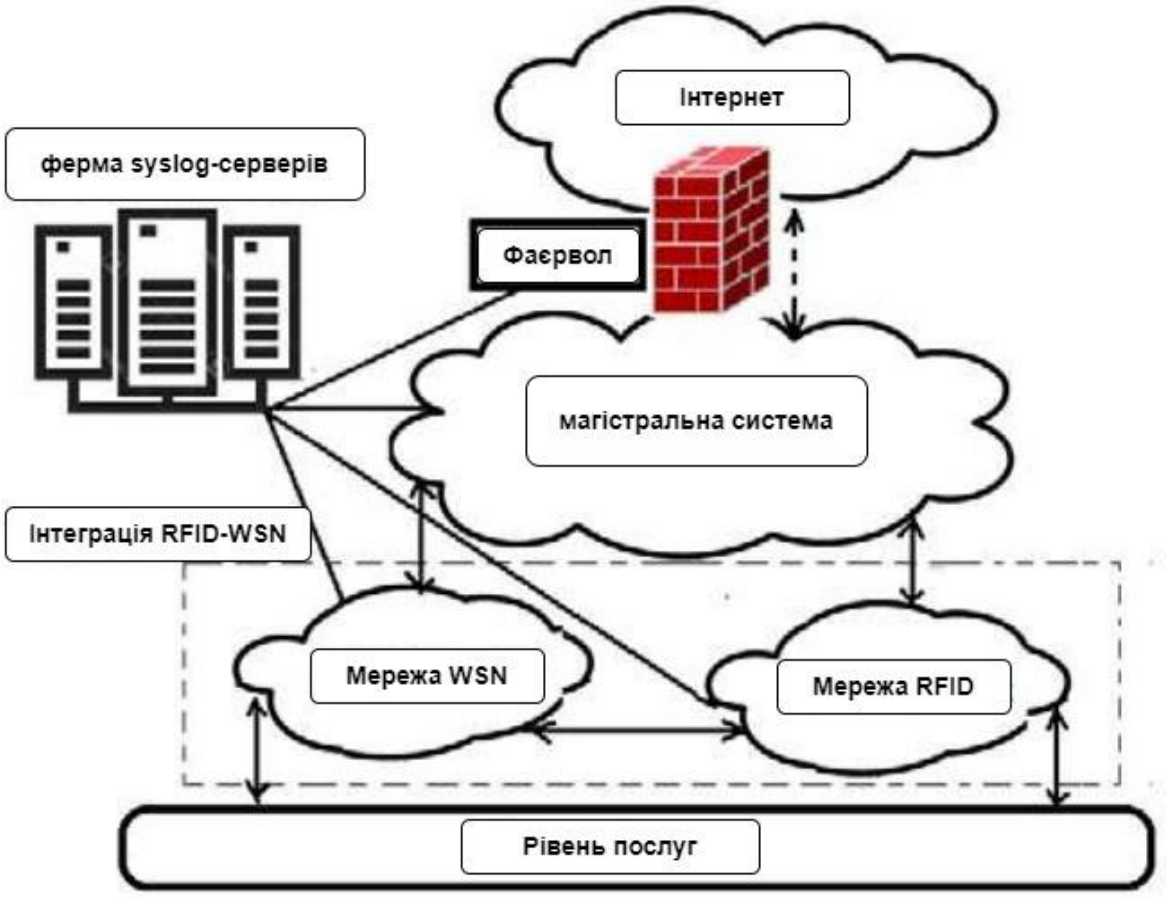

Рисунок 1.4 – Компоненти та базова структура «розумного міста» які можуть бути мішенню для хакерів

Якщо зловмисник збирається дістатися до підрівня послуг ззовні, він повинен перетнути щонайменше три рівні, такі як надійний брандмауер, магістраль, інтегрована мережа WSN-RFID, шлюз і, нарешті, рівень послуг і застосунки. У цьому напрямку правильна конфігурація на різних етапах може стати перешкодою для зловмисника, в той час як серверний центр системного журналу відстежує всі дозволені і несанкціоновані шляхи і переміщення.

Вимоги до безпеки на цьому рівні повинні включати:

1) Загальний захист системи

Сюди входять вимоги безпеки для кожного рівня, такі як: доступність, захист ключів, цілісність, конфіденційність, ідентичність, процес автентифікації, встановлення довіри.

2) Конфігурація брандмауера

Набір застосунків контролює функції (площина управління). Рекомендовано реалізувати мережевий контроль з метою фільтрації авторизованого та неавторизованого трафіку. Сюди входять такі програми, як брандмауери та балансувальники навантаження. Основні політики, інструкції та списки доступу будуть налаштовані в брандмауерах депутатом парламенту.

3) Моніторинг зв'язку

Зв'язок в «розумних містах» включає в себе безліч комбінацій і мереж доступу до хмарних обчислювальних платформ. Постійний моніторинг трафіку в режимі реального часу та управління ним потребує перевірки функціональних можливостей. Сервери системного журналу можуть зберігати всі треки, пов'язані зі станом зв'язку між магістраллю та інтегрованою системою RFID-WSN, пропускною здатністю, швидкістю та перевіркою трансляції (фальшиві штормові затоплення), конфіденційністю та цілісністю сигналізації, надмірним підключенням, а також зв'язком між шлюзом та верхнім/нижнім рівнями.

4) Моніторинг відмов обладнання

Включає в себе постійне та періодичне обслуговування обладнання, такого як: Брандмауери, кабельні з'єднання, маршрутизатори та магістральні комутатори.

5) Компрометація шлюзів

У «розумних містах» мережеві шлюзи є посередниками між рівнем сприйняття і хмарною системою, отримуючи, агрегуючи, обробляючи, фільтруючи і передаючи сенсорні дані на платформу хмарної системи. Пристрої Інтернету речей виконують процес автентифікації на локальному шлюзі при відправці зібраних даних, і шлюз також повинен реалізувати процес автентифікації до хмарної системи. Зіткнення, глушіння та компрометація шлюзу є наслідком існування чорної діри на шлюзі. Потрібен повний аналіз шлюзів за допомогою звичайних інструментів безпеки в режимі реального часу.

1.5 Соціально-технічна безпеки в розумних містах

Електронна взаємодія між людьми, технологіями та платформами Інтернету речей у розумному місті може викликати серйозні проблеми з безпекою. Захист архітектури IoT від вразливостей може бути здійснений на різних рівнях комунікації. Як було сказано раніше, аутентифікація користувачів є першим і основним кроком захисту в інтелектуальному співтоваристві (сервісний рівень). Вони розглядаються як базовий елемент або агент. Безпека ліній зв'язку між базовими агентами і другим рівнем (мережами WSN і RFID) гарантує зв'язок між усіма об'єктами в розумному місті. Те, що обговорювалося в попередньому розділі, відноситься до гарантії мережевого рівня. Іншими словами, захист RFID і WSN буде основною стратегією в цьому напрямку. Вимоги операційної безпеки розумного міста полягають в тому, щоб гарантувати, що технологія та інфраструктура Інтернету речей захищені від будь-яких кібератак різного рівня. Крім того, ще одне велике занепокоєння пов'язане з генерацією даних і зв'язком між різними елементами платформи. Однак безпека генерації даних та захист системи залежить від безпеки всього мережевого рівня, тому зловмисник може проникнути в систему, порушивши політику доступу до даних у разі наявності будь-якої вразливості [22].

1.6 Висновок до першого розділу

Інтернет речей (IoT) має значний потенціал для покращення різних аспектів життя у «розумних містах», таких як ефективність управління міською інфраструктурою, підвищення якості послуг для громадян та економічна вигода. Проте зростаюча кількість підключених пристроїв викликає занепокоєння щодо безпеки, конфіденційності та довіри до таких систем.

Для успішного впровадження IoT у міській інфраструктурі необхідно забезпечити високий рівень безпеки та надійності на всіх рівнях архітектури IoT – від фізичних пристроїв до програмних застосунків. Це включає розробку захищених мережевих архітектур та протоколів, які можуть протидіяти кіберзагрозам та захищати конфіденційність даних користувачів.

Довіра користувачів до систем IoT є критично важливою для їх успішного прийняття та використання. Надійність систем, безпечний обмін даними та захист приватної інформації є основними факторами, що впливають на довіру громадян до технологій IoT.

Дослідження показують, що для побудови ефективних та безпечних «розумних міст» необхідно застосовувати інноваційні підходи до розробки IoT архітектур і протоколів. Це забезпечить не тільки підвищення якості життя громадян, але й створить основу для сталого розвитку міської інфраструктури в майбутньому.

2 МЕТОДОЛОГІЯ ЗАХИСТУ АРХІТЕКТУРИ «РОЗУМНИХ МІСТ»

2.1 Виклики безпеки та конфіденційності в архітектурах IoT

При проектуванні архітектури РМ виникає багато проблем, і найважливіші з них пов'язані з тим, що системи IoT складаються з дуже великих гетерогенних мереж як з обмеженими, так і з необмеженими пристроями, які безперервно працюють переважно без будь-якого джерела живлення. Звідси можна припустити, що основними факторами, які забороняють включення потужних механізмів безпеки та конфіденційності в систему IoT, є [23, 24]:

– неоднорідність задіяних систем і пристроїв з точки зору комунікаційних технологій, програмного забезпечення, апаратних засобів і можливостей;

– обмеженість багатьох пристроїв IoT, які можуть мати дуже обмежені ресурси;

– потреба в масштабованих рішеннях для належного функціонування навіть при великомасштабному розгортанні;

– необхідність енергоефективної оптимізації як апаратного, так і програмного забезпечення, щоб пристрої могли працювати без необхідності заміни батарей протягом тривалого часу.

Ці виклики можуть створювати серйозні труднощі при розробці архітектури, яка б забезпечувала безпеку і конфіденційність, і особливо при спробі вбудувати функції безпеки і конфіденційності на пристроях з обмеженими ресурсами. У [25] було проаналізовано вразливості існуючих апаратних пристроїв Інтернету речей, і висновки виявилися дуже тривожними. Основними результатами цього звіту було те, що понад 90 % пристроїв збирали особисту інформацію, 70 % з них використовували незашифрований трафік, а 60 % використовували слабкі облікові дані. Очевидно, що незалежно від того, наскільки захищеною є магістральна система Інтернету речей, відсутність безпеки на пристроях може скомпрометувати всю систему, і це необхідно серйозно враховувати при розробці безпечних архітектур Інтернету речей.

Архітектура систем IoT розроблена таким чином, щоб мінімізувати ризики атак або збоїв. Насправді, в системі IoT можуть бути як людські, так і нелюдські

джерела ризику. Людські ризики пов'язані з тим, що зловмисники можуть зламати пристрої та викрасти інформацію, або коли помилки чи нещасні випадки користувачів впливають на продуктивність системи. Нелюдський ризик виникає, коли проблеми з безпекою виникають через природні явища, наприклад, повінь, пожежа, спека або апаратна несправність пристрою.

Зазвичай розробники систем розглядають лише людські джерела ризику і, в основному, навмисні зловмисні атаки, вважаючи, що всі інші джерела ризику знаходяться поза сферою їхнього впливу. Однак, використовуючи IT-технології, вплив багатьох інших ризиків також можна пом'якшити. Наприклад, коли надійність даних розраховується для того, щоб відкинути помилкові вимірювання, дані, зібрані пристроєм, який постраждав від збою або пожежі, можуть бути визначені як помилкові і не враховані в системних рішеннях. Крім того, коли пристрої постраждали від повені і не надсилають вимірювання, належні механізми моніторингу можуть створювати сповіщення, щоб оператор системи міг вирішити проблему і відновити роботу пристроїв.

Як описано в [26, 27], для розробки безпечної архітектури IoT, в якості першого кроку необхідно визначити елементи (або активи), які потрібно захистити в системі IoT. Загалом, основні елементи, що підлягають захисту, можна розділити на ті, що базуються на IT, і ті, що не базуються на IT:

– Елементи, що базуються на IT: ця категорія включає такі активи, як облікові дані користувача/пристрою, різні типи даних, якими обмінюються в системі (дані користувача, дані з давачів або дані активації, дані застосунків, дані управління), а також програмне забезпечення.

– Не-IT-елементи: ця категорія є більш загальною і включає такі елементи, як: користувачі-люди, пристрої (майнд- чи посередники), конфіденційність користувачів, послуги, канал зв'язку та в цілому інфраструктура.

Для ідентифікації ризиків в системах IoT та оцінки їх впливу можна використовувати стандартні методології, такі як STRIDE/DREAD від Microsoft [11] або аналіз конфіденційності, наявності цілісності на активах та загроз аутентифікації, авторизації та обліку, а також загроз конфіденційності.

Після ідентифікації ризиків наступним кроком є визначення системних вимог для того, щоб мати можливість пом'якшити ці ризики, і, особливо, вибір дизайну, який повинен зробити оператор або розробник системи для того, щоб забезпечити безпеку і захист своєї системи і своїх даних. У деяких випадках розробнику системи доводиться приймати складні, але важливі рішення, оскільки безпека/ приватність і функціональність/ гнучкість/ інтероперабельність/ відкритість можуть бути суперечливими вимогами. Наприклад, одним з головних ворогів конфіденційності є зв'язність даних, яка в основному необхідна для поліпшення інтероперабельності системи IoT. Крім того, сильна безпека досягається за рахунок продуктивності системи через високу складність для запуску, тобто потужні механізми шифрування на пристроях. Однак рівень безпеки, конфіденційності та продуктивності може бути динамічним, обраним на етапі експлуатації, щоб він відповідав можливостям пристрою/системи та вимогам застосунків, які забезпечуються системою. Останнє є дуже важливою вимогою, яку необхідно враховувати, оскільки застосунки можуть мати дуже різні вимоги до безпеки і продуктивності, і належна система IoT повинна мати можливість адаптуватися до цих різноманітних вимог. Наприклад, додаток для моніторингу навколишнього середовища може мати дуже низькі вимоги до безпеки і продуктивності, в той час як інтелектуальний додаток для охорони здоров'я буде мати високі вимоги до безпеки, конфіденційності та продуктивності. Таким чином, системи Інтернету речей через вимогу до інтероперабельності та подолання ізоляції повинні бути достатньо розумними, щоб без проблем підтримувати обидва ці застосунки.

2.2 Висновок до другого розділу

Розробка архітектури Інтернету речей (IoT) для «розумних міст» стикається з численними викликами, зумовленими гетерогенністю систем, обмеженими ресурсами пристроїв, потребою у масштабованості та

енергоефективності. Для успішного впровадження IoT необхідно подолати ці виклики, особливо в контексті забезпечення безпеки та конфіденційності.

Аналіз показує, що більшість існуючих пристроїв IoT мають серйозні вразливості, такі як збір особистої інформації, використання незашифрованого трафіку та слабкі облікові дані. Ці вразливості підкреслюють важливість інтеграції потужних механізмів безпеки на всіх рівнях системи IoT, починаючи з фізичного рівня і закінчуючи застосунками.

Основними джерелами ризику для IoT є як людські, так і нелюдські фактори. Зловмисні атаки, природні катастрофи та технічні несправності можуть серйозно вплинути на роботу системи. Тому розробка надійних механізмів моніторингу та управління ризиками є ключовою для забезпечення стабільності та безпеки IoT. Визначення елементів, які потребують захисту, та ідентифікація ризиків є першими кроками у процесі розробки безпечної архітектури IoT. Для цього використовуються стандартні методології, такі як STRIDE/DREAD, що дозволяють оцінити загрози і розробити відповідні заходи для їх пом'якшення.

Також, необхідно враховувати динамічність вимог до безпеки, конфіденційності та продуктивності, що залежать від специфіки застосунків IoT. Системи повинні бути достатньо гнучкими, щоб адаптуватися до цих вимог і забезпечувати інтероперабельність між різними застосунками. Це дозволить створити безпечну, надійну та ефективну IoT-інфраструктуру, що відповідає потребам «розумних міст».

3 БЕЗПЕЧНІ АРХІТЕКТУРИ «РОЗУМНОГО МІСТА»

Проведемо аналіз ключових проектів у сфері «розумних міст» і їх елементів на базі Інтернету речей, які впровадили в свої архітектури функції безпеки, конфіденційності та довіри.

3.1 Архітектури «розумних міст»

3.1.1 IoT-A

Метою проекту «Архітектура Інтернету речей» (IoT-A) було створення основ для розробки архітектурної еталонної моделі (ARM) для IoT. Проект був спрямований на створення узгодженої архітектури, яка дозволяє інтегрувати різнорідні технології та підтримує інтероперабельність систем IoT. IoT-A окреслив принципи та рекомендації щодо технічного проектування протоколів, інтерфейсів та алгоритмів зв'язку та надання послуг IoT. Крім того, IoT-A запропонував інноваційну інфраструктуру вирішення сервісів для масштабованого виявлення ресурсів та об'єктів реального світу.

Діяльність IoT-A ґрунтувалася на концепції, що ключовим аспектом будь-якої системи Інтернету речей є «речі» та «комунікація» між ними. На відміну від багатьох попередніх підходів, які використовували термін «речі» для позначення сенсорних пристроїв, IoT-A визначила, що «речі» - це фізичні об'єкти (ФО), які знаходяться навколо нас і до яких ми отримуємо доступ через пристрої. Речі, які підключені до інтернету, це, таким чином, кімната, ручка, холодильник, автомобіль, місто, ноутбук, все, що є фізичним об'єктом і представляє інтерес для користувача. Ці фізичні об'єкти перетворюються на віртуальні об'єкти (ВО), щоб їх можна було шукати, визначати місцезнаходження та контролювати за допомогою програмного забезпечення. Концепція віртуалізації допомагає приховати гетерогенність пристроїв і приховати пристрої з точки зору застосунків, так що користувачі запитують тільки дані для ФО і не повинні знати, які пристрої контролюють або керують цим ФО. Цей підхід до сервіс-

орієнтованої архітектури використовує ресурси на пристроях IoT, які доступні через сервіси, що можуть бути повторно використані багатьма застосунками або можуть бути скомпоновані для надання більш складних послуг [28].

Що стосується безпеки та конфіденційності, IoT-A визначив багато системних вимог, як функціональних, так і нефункціональних, які допомогли в розробці ARM. Вимоги були розділені на три основні категорії:

Надійність системи: ця категорія включає вимоги щодо підвищення загальної безпеки системи IoT та її інфраструктури. Вона включає в себе вимоги до:

– Доступності послуг та інфраструктури, щоб користувач міг звернутися до послуги за будь-яких умов, а інфраструктура повинна бути здатна надавати цю послугу в будь-який час.

– Підзвітність, щоб будь-які збої або неправильна поведінка могли бути відстежені до відповідальної особи/системи.

– Інфраструктурна цілісність і довіра, щоб надані інфраструктурні послуги заслуговували на довіру і могли працювати відповідно до своїх проектних вимог.

– Неможливість відмови, щоб до всіх послуг могли отримати доступ їхні законні власники.

– Комунікаційний стек: ця категорія включає вимоги до мережевого рівня та рівня послуг:

– Мережевий рівень: тут вимоги пов'язані з анонімізацією на мережевому рівні, щоб користувачі могли захистити свою приватність через анонімність, і конфіденційністю, щоб повідомлення були зашифровані для захисту від підслуховування.

– Рівень послуг: тут вимоги пов'язані з автентифікацією послуг і контролем доступу, щоб тільки автентифіковані користувачі могли мати доступ до системних послуг і навіть більше - тільки до певних послуг, які їм дозволені, і довірою до послуг і репутацією, щоб тільки автентифіковані користувачі мали доступ до системи і тільки довірені вузли могли проводити вимірювання.

Конфіденційність користувачів і послуг: ця категорія включає вимоги або щодо захисту користувачів під час використання ними Послуг та Інфраструктури, або щодо неможливості отримання користувачами інформації про суб'єкта даних, який надає певну послугу.

Щоб задовольнити попередні вимоги, IoT-A визначив ряд компонентів безпеки, які повинні бути включені в архітектуру. Архітектуру IoT-A, яка називається ARM, та відповідні функціональні групи (ФГ). Оскільки ця глава присвячена лише компонентам безпеки та конфіденційності архітектури IoT, ми обмежимося описом відповідних ФГ безпеки та управління, тоді як опис решти ФГ опускається.

ФГ «Управління» включає в себе, серед іншого, функціональні можливості, які можуть підвищити відмовостійкість і доступність системи в цілому. Наприклад, компонент «Несправність» може ідентифікувати та виправляти системні несправності, виявляючи їх шляхом генерування тривог та застосування механізмів виправлення. Сигнали тривоги також можуть бути надіслані іншим компонентам, які повинні діяти, щоб виправити конкретну несправність. Інший компонент, який називається «Учасник», обробляє членство та пов'язану з ним інформацію всіх відповідних суб'єктів системи. Він включає в себе базу даних, яка зберігає інформацію про власність, правила, права і т.д., і є важливою для Security FG для визначення політики безпеки і конфіденційності [29].

Security FG - це основна група функціональних можливостей для забезпечення безпеки та конфіденційності системи, що включає наступні компоненти [30]:

– Авторизація: обробляє політики безпеки та приймає рішення щодо контролю доступу на основі цих політик. Вона визначає, чи дозволена та чи інша дія користувача, і контролює політики для послуг, додаючи, оновлюючи або видаляючи політики відповідно до угод про рівень обслуговування або вподобань користувача.

– Автентифікація: передбачає автентифікацію як для користувачів, так і для служб. Вона перевіряє облікові дані, і якщо вони дійсні, то дозволяє доступ до сервісів IoT.

– Управління ідентифікацією: вирішує питання конфіденційності, розподіляючи і керуючи псевдонімами і додатковою інформацією для довірених суб'єктів, щоб вони могли працювати анонімно.

– Обмін та управління ключами: забезпечує механізми для безпечного зв'язку між двома або більше вузлами системи. Він також відповідає за безпечний розподіл ключів для захищених комунікацій, а також за реєстрацію можливостей безпеки.

– Архітектура довіри та репутації: цей компонент збирає та оцінює оцінки репутації користувачів, щоб використовувати їх для розрахунку рівня довіри до сервісу. Це робиться шляхом запиту інформації про репутацію у користувачів щодо сервісу і надання репутації сервісу зацікавленим застосункам або користувачам.

Загалом, IoT-A заклав основи архітектури систем IoT, і в запропонованому ARM були включені деякі базові функції для забезпечення безпеки і конфіденційності. Ці функції можна охарактеризувати як необхідний мінімум, який може включати в себе система IoT, щоб її можна було визнати безпечною.

3.1.2 iCore

Проект «Розширення можливостей Інтернету речей за допомогою когнітивних технологій» (iCore) має на меті забезпечити світ Інтернету речей необхідними технологічними основами для розширення можливостей Інтернету речей за допомогою когнітивних технологій, щоб послуги та застосунки Інтернету речей могли бути легко і просто поширені. iCore структурувала це бачення для вирішення двох основних питань: як абстрагуватися від технологічної неоднорідності, притаманної об'єктам реального світу, враховуючи велику кількість різноманітних об'єктів, які створюють проблеми з надійністю, енергоефективністю та контекстною обізнаністю, та як врахувати

вимоги різних користувачів та зацікавлених сторін, спрямовані на підтримку цілісності бізнесу та надання застосунків відповідно до угод про рівень обслуговування [31].

Для досягнення цих цілей iCore структурувала когнітивну архітектурну структуру, яка включає три рівні функціональності, що можуть бути повторно використані для різних застосунків: віртуальні об'єкти (ВО), композитні віртуальні об'єкти (КВО) та рівень обслуговування. Віртуальні об'єкти використовуються для подолання технологічної гетерогенності, забезпечуючи когнітивне віртуальне представлення як реального світу (наприклад, стілець, стіл, будинок), так і цифрових об'єктів (наприклад, давач, привід, пристрій). КВО є когнітивним мешапом семантично сумісних ВО і використовують послуги останніх відповідно до вимог користувача або зацікавлених сторін.

Що стосується безпеки та конфіденційності, то iCore визначила відповідні вимоги, враховуючи існуючу нормативну базу (наприклад, директиви ЄС) та три основні сценарії використання проекту. В результаті аналізу цих джерел було визначено п'ять основних вимог до безпеки:

– Доступність, забезпечення достовірності даних, що надсилаються авторизованим користувачам.

– Конфіденційність, забезпечення конфіденційності користувачів та захисту їхніх даних, унеможливлення розкриття інформації неавторизованим особам, пристроям або службам. Ця вимога включає також вимоги щодо анонімізації та псевдонімізації.

– Цілісність, що гарантує коректність роботи системи відповідно до певних заздалегідь визначених правил та узгодженість даних.

– Аутентифікація або авторизація, що гарантує правомірність надання даних/послуг, підтверджуючи повноваження особи на отримання цієї інформації.

– Відмова від відповідальності - запевнення як відправника, так і одержувача інформації в тому, що вона була надіслана правильним відправником і що її отримав правильний одержувач.

Враховуючи ці вимоги, iCore визначила також деякі вимоги більш високого рівня для проектування архітектури [32]. Ці вимоги були пов'язані з функціями безпеки для управління безпекою, масштабованості та багаторівневої безпеки. Мета полягала в тому, щоб механізми і політики безпеки не були статичними і могли регулярно оновлюватися, щоб уникнути використання застарілих облікових даних або зламаного програмного забезпечення. Крім того, механізми безпеки системи повинні бути масштабованими, щоб гарантувати, що вони можуть добре працювати в гетерогенних великомасштабних середовищах. Крім того, вважається, що користувачі iCore мають кілька різних рівнів доступу, облікових даних і захисту даних, і фреймворк повинен бути здатним належним чином обробляти ці різноманітні функції.

Архітектура iCore має на меті диференціювати проект, дозволяючи системі отримувати знання з використання контексту, щоб застосунки могли досягати своїх цілей і розумно поводитися та організовувати власні ресурси системи. Основною концепцією iCore є пізнання через «віртуалізацію», що дозволяє виконувати такі операції, як функціональне збагачення, спрямоване на віртуалізацію з максимальною точністю керованих об'єктів реального світу, які співіснують з віртуальними функціональними просторами, абстрагування, що дозволяє узагальнити функціональні можливості, щоб їх можна було застосувати до більшого набору ситуацій і вимог, і агрегування, що дозволяє поєднувати віртуальні об'єкти з можливостями динамічного розуміння контексту, щоб вони забезпечували функціональні можливості більш високого рівня, близькі до реальних потреб світу.

Для забезпечення підвищеної безпеки системи в запропонованій архітектурі iCore є група функціональності для управління безпекою, яка включає в себе репозиторій політик, провайдера ідентифікації та точку прийняття рішень щодо політики (PDP) [33]. На всіх рівнях є компоненти Policy Enforcement Point для перехоплення будь-якого запиту на нову послугу або на виконання ВО або КВО. Потім ці запити надсилаються до Policy Enforcement Point, який оцінює запити відповідно до попередньо визначених політик безпеки і повертає результати. Таким чином в системі iCore забезпечується належна

автентифікація та контроль доступу. Ці функції забезпечуються в iCore за допомогою інструментарію безпеки на основі моделей (SecKit), який є основою для інженерії безпеки, захисту даних і конфіденційності. Він містить мета-моделі, які підтримують моделювання даних, ідентифікаторів, контексту, довіри, ризиків і правил політики.

Архітектура безпеки iCore може забезпечити функціональність для:

– Управління довірою, використовуючи політики безпеки, які враховують довірчі відносини, встановлені користувачами з пристроями та операторами.

– Динамічна адаптація контексту, завдяки чому будь-які зміни контексту будуть враховуватися в діях безпеки.

– Конфіденційність даних через: анонімізації даних, щоб дозволити правилам конфіденційності забезпечити належну анонімізацію даних, коли вони збираються пристроями, а також контроль потоку даних від пристроїв, щоб дозволити користувачам визначати, які дані і якого типу будуть збиратися пристроями.

– Контроль дій виконавчих механізмів, щоб підвищити безпеку системи.

3.1.3 BUTLER

Проект BUTLER спрямований на підтримку розробки повсюдних застосунків з використанням гетерогенних пристроїв, протоколів і стандартів. Застосунки створюються з метою покращення повсякденної діяльності користувачів у різних сферах, враховуючи, серед іншого, контекстну інформацію, якою можуть бути потреби та вподобання користувачів, їхнє місцезнаходження або статус фізичних об'єктів, з якими вони взаємодіють. Архітектура BUTLER була побудована на існуючих стандартах та галузевих ініціативах, таких як IoT-A та FI-WARE [34]. Однак архітектура BUTLER включає в себе додаткові функціональні можливості, пов'язані з прив'язкою контексту до віртуальних сутностей.

Що стосується безпеки та конфіденційності, BUTLER, як і iCore, зосередився на контекстно-орієнтованій безпеці, адаптуючи свої механізми,

використовуючи вхідні дані з навколишнього середовища з урахуванням будь-яких змін, які можуть відбутися, з метою використання цієї інформації для запобігання неналежній поведінці [35]. Були розроблені механізми управління доступом на основі контексту, для прийняття рішення про те, чи буде задоволений запит на доступ до ресурсу або до певних даних, чи відхилений. BUTLER розглянув політики безпеки на основі контексту, щоб реакції безпеки системи IoT були адаптовані до контексту їх використання. Ці політики повинні описувати дозволені дії для користувача/суб'єкта системи в кожен момент часу і в кожній ситуації. Крім того, ці політики використовуються не тільки для контролю доступу, але й для шифрування комунікацій та інших функцій безпеки. Окрім контекстно-орієнтованої безпеки, BUTLER також зосередився на підвищенні конфіденційності користувачів [36]. BUTLER вважає, що застосунки можуть створювати проблеми конфіденційності з точки зору використання даних, зібраних пристроями.

Архітектура BUTLER передбачає чотири основні рівні:

– Комунікаційний рівень, що включає всі функціональні можливості для забезпечення зв'язку між різнорідними пристроями та між різними об'єктами системи і користувачами. Крім того, він включає різні служби безпеки для автентифікації та авторизації пристроїв і користувачів, щоб гарантувати, що тільки ідентифіковані та авторизовані пристрої можуть приєднатися до мережі BUTLER.

– Рівень управління даними/контекстом, який обробляє всі функції, пов'язані з даними і контекстом (наприклад, захоплення і збір даних, постійне зберігання, обробка даних, витяг контексту і т.д.), але не включає жодних служб безпеки.

– Рівень управління системою/пристроєм займається управлінням і обслуговуванням великої кількості різнорідних мережевих пристроїв. Цей рівень має прямі інтерфейси зі службами безпеки, тобто для забезпечення безпечної конфігурації пристроїв, санкціонованого управління ними тощо.

– Рівень сервісів відповідає за опис, виявлення, зв'язування та надання контекстно-залежних сервісів BUTLER. Він також відповідає за те, щоб зробити

ці сервіси доступними для застосунків, надаючи засоби для підтримки виявлення і придбання функціональних можливостей даних.

Як видно, основні функції безпеки та конфіденційності BUTLER знаходяться на комунікаційному рівні, який забезпечує доступ користувачів до всіх інших функцій. Служби безпеки BUTLER побудовані навколо потужного сервера авторизації. Основними послугами безпеки є:

– Безпечна передача повідомлень між пристроями та сервером авторизації, що базується на захисті транспортного рівня (TLS).

– Аутентифікація користувачів і застосунків з використанням облікових даних.

– Реєстрація та автентифікація ресурсу, включаючи інформацію про те, які дії дозволено виконувати на цьому ресурсі його споживачам.

– Управління ключами, як для ключів шифрування, так і для ключів авторизації.

– Наскрізний захист між користувачем програми та постачальником Ресурсу.

– Автентифікація пристроїв за допомогою механізму бутстрапінгу між пристроями та шлюзами на рівні сенсорної мережі з використанням асиметричної криптографії та еліптичних кривих.

Як очевидно, основна увага BUTLER зосереджена на забезпеченні безпеки та конфіденційності на рівні комунікації, при цьому багато функцій побудовано навколо потужної системи автентифікації та авторизації. Це дуже важливо для того, щоб забезпечити доступ до послуг і приватної інформації лише уповноваженим особам, уникаючи розголошення інформації третім особам.

3.1.4 OpenIoT

OpenIoT сфокусований на розробці проміжного програмного забезпечення IoT з відкритим вихідним кодом для отримання інформації з гетерогенних сенсорних мереж, приховуючи типи пристроїв, які надають цю інформацію. OpenIoT приймає концепції IoT-A «сутностей» і ресурсів, таких як давачі,

виконавчі механізми та інтелектуальні пристрої, використовуючи їх для побудови концепції «зондування як послуги» за допомогою адаптивного проміжного програмного забезпечення для розгортання та надання послуг у хмарних середовищах [37].

Архітектура OpenIoT побудована на основі різних нефункціональних вимог для підвищення продуктивності, масштабованості, надійності, конфіденційності та безпеки. Проект визнає, що надана платформа повинна бути безпечною і зберігати конфіденційність. У зв'язку з цим розробляються механізми рольової автентифікації та авторизації, на основі яких надаються механізми конфіденційності, керовані утилітами.

Архітектурні компоненти OpenIoT, відображені на IoT-A ARM. Ця архітектура включає, серед іншого, групу компонентів безпеки, що забезпечують в основному функції авторизації, управління ідентифікацією та автентифікації. Як описано в [38], платформа OpenIoT складається з декількох автономних застосунків, таких як X-GSN, LSM тощо, які потребують власних механізмів безпеки. Через розподілену природу платформи, OpenIoT визнав важливість проектування та розробки централізованого сервера авторизації, який би надавав послуги аутентифікації та авторизації для всіх компонентів системи. OpenIoT визнав, що головною особливістю платформи є те, що облікові дані користувача перевіряються і підтримуються тільки цим центральним сервером, а потім цей сервер виконує авторизацію застосунків, які запускаються від імені користувача. Таким чином, облікові дані користувача не поширюються між різними компонентами, що покращує конфіденційність системи.

Що стосується безпеки зв'язку, то для магістральних комунікацій (між шлюзами і хмарними серверами) використовуються такі механізми, як TSL або HTTPS. На сенсорному рівні використовуються стандартні механізми безпеки IEEE 802.15.4. Для авторизації використовується OAuth, оскільки це відкритий стандарт, який може бути легко інтегрований у відкриту платформу. Крім того, OpenIoT розробив також фреймворк для оцінки достовірності показань давачів за допомогою просторової кореляції вимірювань. У цьому відношенні показання

сусідніх давачів корелюються для оцінки їх достовірності та відкидання недостовірних показань [39].

3.1.5 SMARTIE

SMARTIE (Secure and Smarter Cities Data Management) має на меті створити основу для застосунків Інтернету речей, які обмінюються великими обсягами різнорідних даних. Основна увага приділяється забезпеченню наскрізної безпеки та довіри до інформації, враховуючи також вимоги щодо збереження конфіденційності користувачів. Механізми і технології для забезпечення безпеки і довіри на рівні сприйняття, обслуговування і мережі, а також для безпечного зберігання і контролю доступу займають центральне місце в системі.

Розробка архітектури системи SMARTIE [40] ґрунтувалася на довгому переліку вимог, представленому в Що стосується безпеки та конфіденційності, SMARTIE підтримує обробку інформації на довірених вузлах та анонімність користувачів для захисту приватності, конфіденційності даних, надійного контролю доступу та автентифікації, безпечного зберігання, згоди користувача, контекстно-орієнтованих політик, конфіденційності місцезнаходження, цілісності зв'язку, запобігання несанкціонованому втручанню в роботу пристроїв та відмовостійкості системи.

Архітектура SMARTIE базується на IoT-A ARM, відповідно до методології IoT-A та функціональних груп ARM для організації всіх функціональних компонентів архітектури SMARTE [41]. Існує багато функціональних можливостей, пов'язаних з безпекою, не тільки у ФГ безпеки, але й вбудованих в інші ФГ. Наприклад, компонент «Розподіл даних IDS» сканує мережевий трафік на наявність зловмисників і повідомляє про небажаний або невідомий трафік оператору мережі, розподіляючи виявлені події на інші пристрої. Крім того, компонент «Каталог ресурсів із захищеним сховищем» забезпечує безпечний доступ до наявних в системі ресурсів, дозволяючи також їх безпечне зберігання. Компонент «Privacy-preserving Geofencing» пропонує безпечні сервіси на основі визначення місцезнаходження з використанням захищеної

геофіксації, щоб уникнути розголошення інформації про місцезнаходження користувачів неавторизованим особам.

У ФГ «Безпека» SMARTIE надає наступні компоненти та функції:

– - Авторизація, заснована на DCapBAC, для забезпечення того, щоб рішення про контроль доступу приймалися до того, як користувач отримає доступ до послуги. Контроль доступу на основі атрибутів з використанням фреймворку XACML/JSON, що використовує політики для вираження багатих і деталізованих рішень щодо контролю доступу.

– Цілісність системи на основі атестації вузлів (IMASC). IMASC забезпечує надійне середовище для більшості вбудованих пристроїв, що використовують смарт-карти, дозволяючи виявляти шкідливий код або неправильні вимірювання.

– Аутентифікація з використанням розподіленого Kerberos і симетричної криптографії.

– Шифрування на основі схеми CP-ABE [42], яка шифрує інформацію на основі політик.

– - Бібліотеки для shortECC та LmRNG, щоб забезпечити еліптичні криві з довжиною ключа від 32 до 64 біт та генерувати криптографічно безпечні псевдовипадкові числа відповідно.

SMARTIE також слідує концепції IoT-A, розділяючи пристрої IoT на обмежені та необмежені. З точки зору функціональності, SMARTIE пропонує рекомендований набір функціональних можливостей і технологій, які можуть бути використані як для обмежених, так і для необмежених пристроїв, обґрунтовуючи пропозиції щодо забезпечення того, щоб на обмежених пристроях були вбудовані тільки легкі реалізації технологій.

3.1.6 COSMOS

Проект COSMOS має на меті підвищити стійкість застосунків для «розумного міста» на основі Інтернету речей, дозволяючи речам розвиватися і ставати більш автономними, надійними та розумними. Основна концепція

полягає в тому, що речі матимуть можливість навчатися на основі досвіду інших речей за допомогою ситуативного набуття та аналізу знань. Крім того, COSMOS має на меті забезпечити наскрізну безпеку і конфіденційність, з апаратно-кодованою безпекою і конфіденційністю на сховищі, представляючи концепцію Privetlets для послуг IoT.

Архітектурна структура COSMOS побудована з урахуванням великої кількості вимог до безпеки, конфіденційності та довіри [43]. COSMOS передбачає, що дані повинні бути захищені від підслуховування, атак на модифікацію даних, крадіжок особистих даних або атак на відтворення. Також передбачається, що на пристроях є безпечне сховище для захисту секретної інформації, що пристрої завантажуються або оновлюються у безпечний спосіб. COSMOS розділяє середовище виконання сервісів на дві частини: безпечну частину, в якій виконуються критичні сервіси, і незахищену частину для некритичних сервісів. COSMOS використовує захищений магістральний сервер для управління ключами, їх зберігання та розповсюдження, а також для реєстрації пристроїв. Аутентифікація та контроль доступу також вбудовані в систему.

Поняття довіри також дуже важливе для COSMOS. Визначено модель довіри для забезпечення цілісності та конфіденційності даних, що дозволяє також автентифікацію кінцевих точок і неспростування між будь-якими об'єктами системи. Крім того, КОСМОС розглядає поняття конфіденційності як дуже важливе для захисту приватної інформації користувачів. Передбачається, що конфіденційність підтримується шляхом надання суб'єктам можливості зберігати контроль над своєю приватною інформацією і вирішувати, чи буде вона збиратися, використовуватися або розкриватися іншим суб'єктам.

COSMOS визначив механізми безпеки на різних рівнях. Проект мав на меті забезпечити наскрізну безпеку і конфіденційність за допомогою механізмів безпеки, вбудованих на рівні пристроїв, контролю доступу, шифрування і перехресного застосування на рівні даних, із застосуванням механізмів збереження конфіденційності, коли це доречно. Для визначення архітектури COSMOS за основу було взято IoT-A ARM.

Основні компоненти безпеки архітектури знаходяться у ФГ «Безпека

– Автентифікація та авторизація використовується для автентифікації суб'єктів та управління розподілом їхніх прав доступу.

– Обмін та управління ключами охоплює генерацію, зберігання та розподіл криптографічних ключів на основі протоколу обміну ключами Діффі та Хеллмана [44].

– Hardware Board Communication Accountability вирішує питання підзвітності, відстеження доступу до криптографічних примітивів з метою неспростування, обчислення індексу репутації суб'єкта.

– Криптографічне неспростування забезпечується на основі компонента підзвітності комунікації апаратної плати.

– Контрольна сума забезпечує цілісність пакетів даних, виявляючи та виправляючи бітові помилки.

У решті ФГ є й інші компоненти, які пов'язані з безпекою, конфіденційністю та довірою

– Привлетлети діють як фільтри, щоб гарантувати, що кожна віртуальна сутність і кожен користувач ділиться лише мінімальною необхідною інформацією, опускаючи всю іншу непотрібну інформацію з метою збереження конфіденційності.

– Канал зв'язку між віртуальними одиницями або між віртуальними одиницями і системою COSMOS повинен бути захищений, тому застосовується шифрування даних, що передаються в цих каналах.

Загалом, COSMOS приділяє велику увагу забезпеченню конфіденційності шляхом мінімізації даних на рівні проміжного програмного забезпечення, а також надійній аутентифікації та авторизації. Шифрування на каналі зв'язку також є важливим для забезпечення конфіденційності даних.

3.1.7 COMPOSE

Проект COMPOSE розробив IoT-платформу, яка полегшує завдання розробників, що пишуть засосунки на основі Інтернету речей (IoT) [45].

Складено абстракції з IoT-пристроїв, присвоївши їм віртуальну ідентичність. Пристрої, які не підключені безпосередньо до Інтернету (наприклад, пляшка вина з міткою RFID або NFC), потребуватимуть проксі для представлення їх на платформі COMPOSE. Об'єкти IoT з мережевими можливостями, але без підтримки мережевих протоколів, необхідних для COMPOSE, такі як прості давачі, також будуть використовувати проксі-сервери для зв'язку з платформою COMPOSE. Нарешті, існує група просунутих пристроїв (так звані «розумні об'єкти», такі як смартфон, планшет або пристрій Arduino), які здатні спілкуватися з платформою COMPOSE напряму. Всі вищезгадані фізичні об'єкти в COMPOSE називаються веб-об'єктами (Web Objects) і представлені як сервісні об'єкти (Service Objects). COMPOSE визначає API, за допомогою якого він планує взаємодіяти з веб-об'єктами, щоб отримати від них дані або встановити дані в них. Сервісний об'єкт надає стандартний API також внутрішньо по відношенню до решти компонентів платформи COMPOSE. Цей API необхідний для того, щоб впорядкувати і стандартизувати внутрішній доступ до сервісних об'єктів, які, в свою чергу, можуть представляти собою безліч дуже різних веб-об'єктів, що надають дуже різні можливості.

Платформа COMPOSE, прагнучи охопити якомога більше транспортних засобів IoT, дозволяє веб-об'єктам взаємодіяти зі своїми представниками на платформі (сервісними об'єктами) за допомогою набору добре відомих протоколів: HTTP, STOMP через TCP, STOMP через WebSockets та MQTT через TCP. На основі сервісних об'єктів COMPOSE пропонує розробляти застосунки. Розробники знаходять цікаві існуючі сервісні об'єкти або застосунки і створюють навколо них специфічну логіку. Крім того, будуть надані рекомендації щодо вибору найкращого сервісного об'єкту на основі потреб розробника та запропонованої композиції, а також рекомендації, засновані на знаннях про платформу, наприклад, аспектах, пов'язаних з безпекою.

Архітектура безпеки COMPOSE базується на підході до вимог безпеки, орієнтованих на дані. Він відрізняється від класичних підходів, орієнтованих на пристрої, тим, що система безпеки COMPOSE звужує периметр безпеки до гранулярності даних. Вона є дрібнозернистою і може поєднуватися зі статичним

і динамічним примусом, щоб відновити управління пристроями і даними без шкоди для внутрішньої відкритості платформ Інтернету речей.

Фреймворк включає в себе наступні концепції:

– Метадані безпеки зберігаються разом з об'єктами, на які вони посилаються. Метадані фіксують політики безпеки користувачів, що визначають рівень конфіденційності, який система повинна підтримувати для них. Сервіс-орієнтовані метадані також дозволяють розробникам і провайдерам визначати використання сервісів або сервісних об'єктів. Метадані будуть використовуватися для ефективного створення безпечних застосунків і робочих процесів, а також для зберігання інформації про походження даних, що генеруються і обробляються в COMPOSE, і для зберігання інформації про репутацію користувачів, сервісних об'єктів і застосунків COMPOSE.

– Інформація про походження генерується виключно системою COMPOSE. Вона архівує інформацію про те, коли, хто і як використовував об'єкт. Вона накопичує інформацію про застосунки, які генерують певні дані, застосунки, які їх споживають, і можливі операції, що виконуються з цими даними, наприклад, їх поєднання з іншими даними або трансляція у віддалені місця за межами системи COMPOSE. Для збору точної інформації про походження даних виконується моніторинг під час диспетчеризації оновлень давачів та виконання застосунків. Менеджер походження даних відстежує походження даних, операції, які над ними виконувалися, і час, коли ці операції відбувалися. Це дозволяє користувачам визначати політики на основі походження даних, наприклад, дозволити об'єкту обслуговування отримувати дані, тільки якщо вони були оброблені певним застосунком. Крім того, візуалізація походження даних може допомогти користувачам виявити, коли виникають певні помилки; наприклад, якщо кілька джерел даних об'єднані, але одне з них несправне, розробник може вивчити джерела правильних значень і порівняти їх з неправильними значеннями, щоб ізолювати несправний пристрій. Крім того, інформація про походження має цікавий потенціал для захисту приватності користувача. Наприклад, вона може допомогти виявити, коли певні

програми збирають і корелюють інформацію від конкретних суб'єктів, натякаючи на можливість профілювання користувачів.

– Інформація про репутацію зберігається у відповідному об'єкті сервісу, а сервіс реєструє зібрані відгуки про об'єкти сервісу та застосунки COMPOSE. Інформацію про репутацію можна збирати як про об'єкти сервісу, так і про популярність застосунку COMPOSE. Компонент під назвою PopularIoTy відображає, як часто певний об'єкт сервісу або додаток використовується, тобто викликається іншими суб'єктами. Щоразу, коли генеруються дані, сповіщення зберігаються у сховищі даних. Крім того, під час виконання розміщуються монітори, які зберігають сповіщення про виклик застосунків. Вся ця інформація обробляється для обчислення показника популярності. Вона також взаємодіє з контрактами для застосунків, так що додаток, який відповідає умовам контракту, отримує позитивну оцінку.

– Контракти для застосунків визначають умови для застосунків, які вказують, коли вони можуть бути виконані безпечно, а також специфікації потоків, які є інформацією про їхні внутрішні, абстрактні потоки даних. У той час як умови визначають стани системи, які повинні бути перед виконанням програми або після її виконання, специфікації потоків надають більше інформації про те, куди, наприклад, до якого ресурсу надходять вхідні дані, а також як і звідки генеруються вихідні дані. Цю інформацію можна згенерувати вручну, описавши критичні послуги безпеки, що надаються COMPOSE, наприклад, шифрування або автентифікацію потоку даних. Після публікації API напівавтоматичний процес генерує контракти на ці API. Ця інформація використовується в розгорнутому середовищі COMPOSE, щоб уможливити і спростити процес аналізу. У загальному випадку, тобто для застосунків, визначених користувачем, контракти генеруються компонентом статичного аналізу ядра безпеки для економії обчислювальних ресурсів під час аналізу робочих потоків COMPOSE.

– Контроль потоків даних забезпечується динамічно і статично. Політика потоку, орієнтована на дані, застосовується до вхідних і вихідних даних для всіх компонентів всередині COMPOSE. Окрім визначення суб'єктів, яким дозволено

доступ, виконання або зміну компонента, політики потоків також описують вимоги до безпеки даних, що надходять до компонента, і властивості безпеки даних, що виходять з нього. Щоб уникнути додаткових витрат на оцінювання, можна використовувати уніфіковану структуру політик, наприклад, у COMPOSE ця мова натхненна ParaLocks [46].

– Управління ідентифікацією здійснюється за допомогою загальної системи IDM на основі атрибутів. Вона пов'язує сутності COMPOSE з ідентифікаторами, зберігає та розповсюджує відповідну інформацію про безпеку, а також надає послуги автентифікації. У COMPOSE підхід на основі атрибутів дозволяє кожному користувачеві позначати себе або свої об'єкти значеннями атрибутів. Після того, як об'єкти позначені атрибутами, наприклад, маркою пристрою, тег можна використовувати для визначення політики безпеки, наприклад, приймати дані тільки з пристроїв цієї марки. COMPOSE дозволяє користувачам затверджувати інформацію про атрибути залежно від групи, до якої вони належать [47].

– Точки застосування на рівні виконання забезпечують доступ до даних, сервісів або інших ресурсів на основі рішень точки прийняття рішень політики (PDP). COMPOSE в своїй основі охоплює безпеку інформаційних потоків, монітори часу виконання (частина PDP) виявляють і запобігають незаконним потокам - як зазначено користувачем або постачальником об'єктів послуг - під час виконання послуг, що надаються користувачем. PDP керує компонентами аналізу безпеки та інструментарію в COMPOSE, завданням яких є виявлення потенційно зловмисних потоків у застосунках або робочих процесах і їх запобігання або пом'якшення шляхом реконфігурації програмного забезпечення або інструментарію.

На рисунку 3.1 наведено архітектуру безпеки COMPOSE.

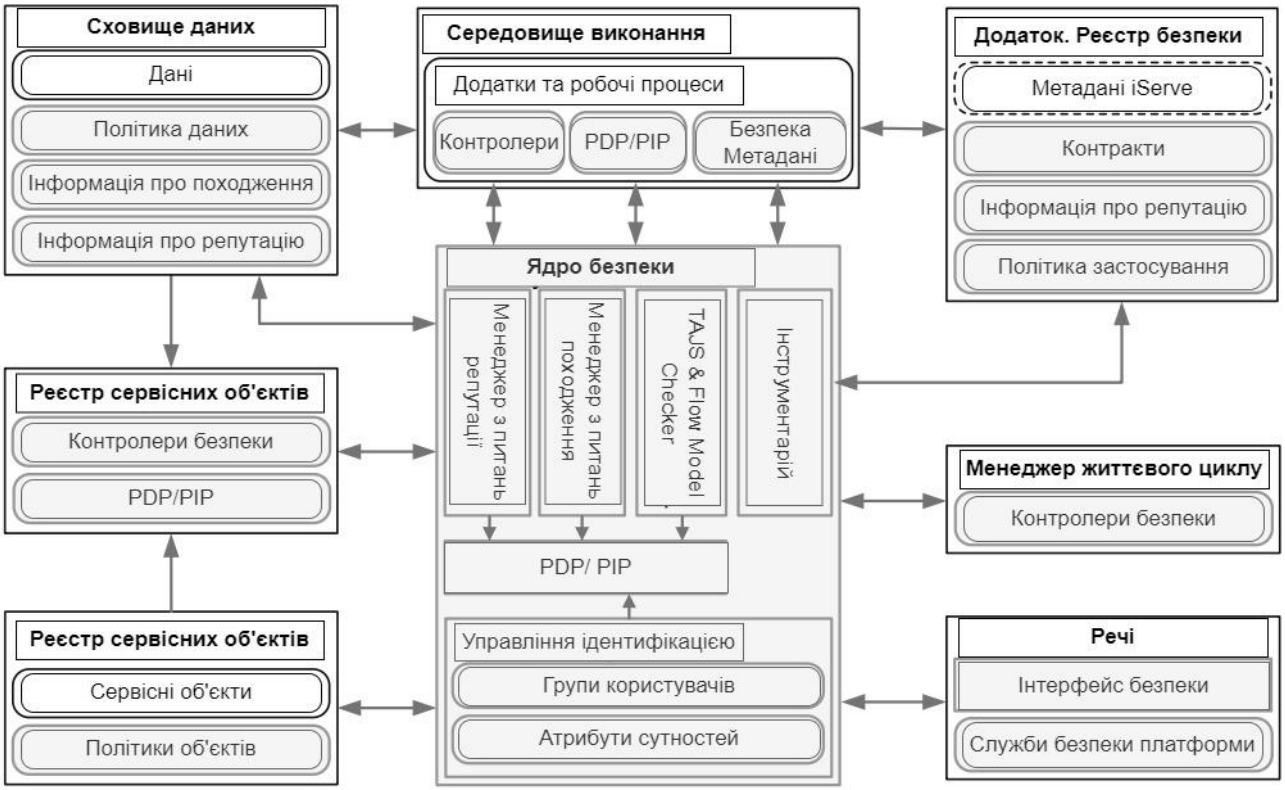

Рисунок 3.1 – Огляд архітектури безпеки COMPOSE.

3.1.8 PRISMACLOUD

Проект PRISMACLOUD - це дослідницький проект, що фінансується ЄС, який розробляє криптографічні інструменти для створення більш безпечних хмарних сервісів, що зберігають конфіденційність. Щоб забезпечити наскрізну безпеку для користувачів хмарних сервісів і надати інструменти для захисту їхньої приватності, проект впроваджує нові криптографічні концепції та методи у практичне застосування [48]. PRISMACLOUD хоче збільшити поширення вже існуючих і, можливо, майже придатних для використання стійких криптографічних примітивів на практиці. На початку проекту цей показник сприймався як низький і тому був визначений як перешкода, що стримує використання менш надійних посередників (таких як хмарні сервіси, шлюзи IoT або проміжне програмне забезпечення IoT) у багатьох сценаріях використання, що враховують безпеку і конфіденційність, наприклад, в «розумних містах». PRISMACLOUD має на меті подолати розрив між необхідними глибокими криптографічними знаннями та прикладними вимогами користувачів хмарних сервісів, щоб криптографічні примітиви знайшли своє практичне застосування.

Архітектура PRISMACLOUD інкапсулює криптографічні знання рівня примітивів всередині інструментів та їх використання всередині сервісів. Вона складається з чотирьох рівнів. Кожен рівень допомагає абстрагуватися від необхідних базових криптографічних примітивів і протоколів, які знаходяться на рівні примітивів, що є найнижчим рівнем архітектури PRISMACLOUD. Побудова інструментів, що знаходяться на рівні вище, з примітивів вимагає глибоких знань з криптографії та розробки програмного забезпечення. Однак після створення вони можуть бути використані розробниками хмарних сервісів для створення криптографічно захищених хмарних сервісів, що зберігають конфіденційність. Таким чином, рівні архітектури PRISMACLOUD також визначають точки зв'язку між різними дисциплінами: криптографами, інженерами/розробниками програмного забезпечення та архітекторами хмарних сервісів. На верхньому прикладному рівні знаходяться застосунки для кінцевих користувачів. Застосунки використовують хмарні сервіси рівня «Сервіси» для досягнення бажаних функцій безпеки. Хмарні сервіси, зазначені там, є репрезентативним вибором можливих сервісів, які можуть бути побудовані з інструментів, організованих на рівні «Інструменти». Зокрема, це спосіб надання інструментів розробникам послуг і архітекторам хмарних сервісів у доступний і масштабований спосіб. Разом ці інструменти складають інструментарій PRISMACLOUD.

Архітектуру PRISMACLOUD можна розглядати як один із способів впровадження криптографічних примітивів і протоколів у хмарні сервіси таким чином, щоб вони давали можливість користувачам хмарних сервісів створювати більш безпечні і більш захищені хмарні сервіси. Зокрема, йдеться про надання інструментів для безпечного зберігання об'єктів, гнучкої автентифікації з вибірковим розкриттям, верифікованої обробки даних, сертифікації топології та конфіденційності даних. Сервіси, розроблені в PRISMACLOUD, включають обмін даними; безпечне архівування; вибірковий автентичний обмін; управління ідентифікацією, що підвищує конфіденційність; статистику, яку можна перевірити; аудит інфраструктури; шифрувальний проксі-сервіс; сервіс анонімізації. Інструменти використовують наступні криптографічні примітиви:

RDC: Віддалена перевірка даних; SSS: Схеми обміну секретними даними; ABC: Облікові дані на основі атрибутів; PIR: Пошук приватної інформації; MSS: Схеми гнучкого підпису; FSS: Схеми функціонального підпису; GSS: Схеми групового підпису; GRS: Схеми графічного підпису; SPE: Шифрування зі збереженням формату та порядку; ZKP: Докази з нульовим знанням; kAN: k-анонімність.

Для прикладу «розумних міст» уявіть собі низку пристроїв Інтернету речей, які постійно записують дані, але не мають засобів зберігання та обчислювальних можливостей для їх агрегації на вищому рівні. Якщо припустити, що ця агрегація буде виконуватися на хмарній інфраструктурі, то цій інфраструктурі необхідно довіряти, щоб вона виконувала обчислення правильно. Тут довіру до цієї інфраструктури можна усунути за допомогою криптографічного примітиву, який називається функціональні підписи. Вони дозволяють делегувати генерацію підписів іншим сторонам для класу повідомлень, що відповідають певним умовам. Такі схеми можна використовувати для сертифікації обчислень, виконаних третіми сторонами, наприклад, ненадійними посередниками, такими як шлюз або проміжне програмне забезпечення стека IoT. На основі цього класу схем підписів PRISMACLOUD створює інструмент обробки даних, який можна перевірити. Інструмент дозволяє виконувати верифіковані обчислення над даними, наприклад, обчислювати статистику на основі даних IoT. [49].

3.1.9 RERUM

RERUM має на меті розробити архітектурну структуру IoT, що базується на концепції «безпеки та конфіденційності за задумом». RERUM визнає, що система IoT не може бути повністю захищеною після розробки, але повинна бути спроектована з самого початку, щоб бути безпечною і зберігати конфіденційність. Це головна відмінність RERUM від інших архітектурних підходів, таких як представлені вище. Процес проектування архітектури RERUM слідував визнаній методології IoT-A, але, крім того, RERUM приділив значну

увагу пристроям IoT. Це було зроблено тому, що RERUM визнає той факт, що до цього часу найслабшим місцем в системі IoT були обмежені пристрої, які не мали можливостей для запуску передових механізмів безпеки та конфіденційності. Дійсно, недостатня увага до безпеки пристроїв призвела до багатьох відкритих дірок у безпеці та конфіденційності, які не обмежувалися лише пристроями, а поширювалися на всю систему в цілому [50].

Окрім нефункціональних вимог до «безпеки та конфіденційності за задумом», RERUM розглянув також вимоги до підвищення надійності, стійкості, відмовостійкості та доступності системи, щоб гарантувати, що система може реагувати на атаки і що дані будуть доступні для надання застосункам, коли вони будуть запитані. Оскільки основна увага RERUM зосереджена на пристроях, ключовим фактором функціональних вимог є те, що розроблені механізми безпеки та конфіденційності повинні бути легкими та енергоефективними, щоб їх можна було легко впроваджувати та вбудовувати навіть на обмежених пристроях Інтернету речей. Вимоги RERUM включають, серед іншого, легке шифрування, захист конфіденційності та цілісності, санкціоновану модифікацію даних, захищених від порушення цілісності, просту і надійну автентифікацію як для користувачів, так і для пристроїв, контроль доступу на основі атрибутів, згоду користувача, обмеження збору даних, мінімізацію даних, підзвітність, безпечне завантаження пристроїв і безпечну конфігурацію пристроїв [36].

Архітектура RERUM пройшла детальний процес визначення та аналізу вимог з метою виокремлення необхідних функціональних компонентів для підтримки довгого переліку вимог. RERUM визначив свої власні функціональні групи, які були названі «менеджерами». Серед інших, RERUM визначив «Менеджер безпеки, конфіденційності та довіри» (SPT), який включає довгий список функціональних компонентів.

Цікавим у цьому відображенні є те, що на відміну від попередніх архітектур безпеки IoT, RERUM розробив велику кількість компонентів, які, як передбачається, будуть вбудовані на пристроях IoT. Наприклад, компоненти для безпечного завантаження облікових даних, безпечного зберігання, методів підвищення конфіденційності геолокації, генератора/верифікатора цілісності,

шифрування/дешифрування даних, довіреної маршрутизації, безпеки когнітивного радіо та автентифікації між пристроями вважаються важливими для запуску на пристроях, щоб забезпечити найвищий рівень безпеки системи IoT за рахунок надійного захисту листових вузлів.

Крім того, компоненти безпеки для автентифікації та контролю доступу також важливі в RERUM, разом з безпечною реконфігурацією пристроїв, створенням та обробкою сповіщень про безпеку, обробкою ідентифікаційних даних користувача та пристрою, а також безпечним зберіганням облікових даних та сертифікатів. Також визначено низку компонентів для забезпечення конфіденційності користувачів за допомогою анонімізації та псевдонімізації, активації та деактивації збору даних на основі уподобань користувача, менеджера згоди для запиту згоди користувача на збір або розкриття приватної інформації, інформаційної панелі конфіденційності, що дозволяє користувачам самим керувати своєю політикою конфіденційності, а також пунктів прийняття рішень щодо політики та її виконання для управління та виконання політик.

Довіра також дуже важлива для RERUM. Проект визначив механізм довіри для обчислення та оцінки рейтингів довіри до пристроїв, сервісів та користувачів на основі спостерігачів, розкиданих по різних об'єктах системи, які відстежують дії користувачів, достовірність даних, зібраних пристроями, та поведінку пристроїв з метою виявлення зловмисних або неправильних пристроїв, щоб вони не впливали на рішення системи. Таким чином, підвищується надійність системи в цілому.

3.2 Компоненти безпечної архітектури Інтернету речей для «розумного міста»

На рисунку 3.2 показані основні компоненти безпечної архітектури Інтернету речей для «розумного міста». Ці основні компоненти включають чорні мережі, довірені контролери SDN (позначені як TTP), єдиний реєстр і систему управління ключами.

Мережі IoT «розумного міста» працюють на основі гетерогенних технологій і з різними типами пристроїв. Базові будівельні блоки безпеки забезпечують безпечний зв'язок і автентифікацію в цих гетерогенних технологіях [51]. Не всі засоби безпеки можуть бути вбудовані у вузли IoT через обмеження ресурсів вузлів IoT. Представимо чотири фундаментальні будівельні блоки безпечної архітектури IoT для розумного міста.

Це: Чорні мережі для захисту даних, конфіденційності, цілісності та автентифікації; Довірена третя сторона (TTP) для ефективної та анонімної маршрутизації через вузли IoT, які сплять до 90% часу; Єдиний реєстр для бази даних пристроїв (давачів, шлюзів і вузлів) та їхніх атрибутів; Управління ключами для зовнішньої системи управління ключами для мереж IoT. У таблиці 3.1 представлено ці сервіси безпеки.

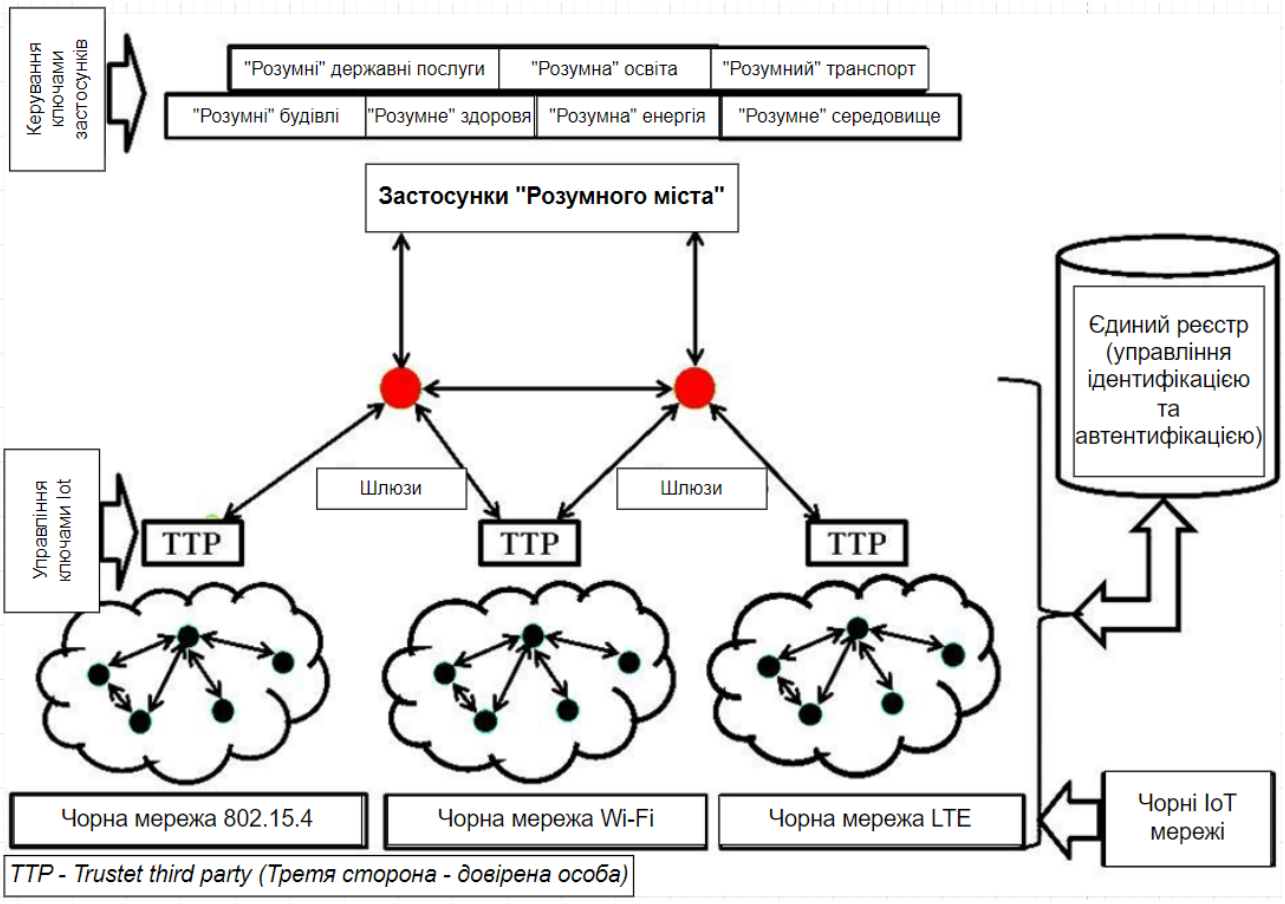

Рисунок 3.2 – Базові компоненти безпечної архітектури Інтернету речей для розумних міст

Таблиця 3.1 – Безпечні послуги з архітектури розумного міста на основі IoT

Безпека розумного міста на основі Інтернету речей	
Компонент безпеки	Служби безпеки
Чорні мережі	Конфіденційність, Чесність, Приватність
Довірений контролер SDN	Безпечна маршрутизація (чорні пакети), Доступність
Єдиний реєстр	Управління ідентифікацією, Аутентифікація вузлів, Авторизація, Облік, Доступність та мобільність
Управління ключами	Керування зовнішніми ключами

3.2.1 Чорні мережі

Чорні мережі - це мережі, які захищають всі дані, включаючи метадані, пов'язані з кожним кадром або пакетом в протоколі IoT [52]. Чорні мережі шифрують корисне навантаження і метадані в протоколі IoT на канальному рівні зв'язку.

Аналогічно, мета-дані незалежно захищаються на мережевому рівні. Шифрування може здійснюватися за допомогою Grain128a або AES в режимах EAX або OFB. Отриманий в результаті сумісний кадр дозволяє одержувачу правильно отримати і декодувати повідомлення, використовуючи спільний секрет.

Чорні мережі пом'якшують широкий спектр як пасивних, так і активних атак, забезпечуючи конфіденційність, цілісність і приватність в мережах IoT завдяки автентифікованим і захищеним комунікаціям як на канальному, так і на мережевому рівнях. Однак шифрування заголовка створює проблеми з маршрутизацією для вузлів IoT, які більшу частину часу перебувають у сплячому режимі.

3.2.2 Довірений SDN контролер

Довірені контролери SDN (Software Defined Networking) керують і організовують потік зв'язку між вузлами Інтернету речей і рештою мережевої інфраструктури. SDN - це мережева парадигма, яка відокремлює потік управління від потоку пакетів даних. Основна мотивація для контролера SDN полягає у вирішенні проблем маршрутизації, що виникають у «чорних мережах» IoT із збереженням конфіденційності [53]. У чорній мережі IoT вузол A бажає відправити пакет на вузол B так, щоб противник не знав, що пакет призначений для вузла B, і пакет від вузла A повинен успішно пройти через мережу IoT, навіть коли вузли сплять більшу частину часу. Ми пропонуємо два загальних методи вирішення цієї проблеми. Контролер SDN, підтримуючи топологію мережі IoT і час сну/пробудження, може заздалегідь визначити маршрут пакета і синхронізувати вузли для маршрутизації. Таким чином, контролер SDN може створювати таблиці потоків для будь-якого чорного пакета, який потрібно направити з вузла A до вузла B, і допомагати в синхронізації часу пробудження для проміжних вузлів. Інший підхід полягає в тому, що контролер SDN створює випадковий, динамічний маршрут для кожного переходу, прокладаючи його через проміжні вузли, що не сплять. Довірений контролер SDN підтримує глобальний огляд мережі IoT, керує циклами сну/пробудження, а також іншими станами мережі.

3.2.3 Єдиний реєстр

Єдиний реєстр використовується для консолідації різнорідних технологій, схем адресації та пристроїв, з яких складаються мережі IoT для розумного міста. Концепція може бути розширена до відвідуваного єдиного реєстру для вузлів IoT, які є мобільними і перетинають мережі. Це важливо з точки зору безпеки, оскільки більшість мереж IoT припускають наявність фіксованих вузлів, що взаємодіють за допомогою бездротових технологій. У середовищі «розумного міста» використовується безліч бездротових технологій (наприклад, WiFi, LTE),

використовується безліч протоколів (наприклад, ZigBee, 6LoWPAN, WirelessHART, Bluetooth Low Energy), а також використовується декілька схем адресації (наприклад, 128-бітна адресація IPv6, 48-бітна адресація Bluetooth, адресація RFID та E.164). Всі ці ідентичності потребують уніфікованого набору атрибутів для управління ідентифікацією, автентифікації, авторизації та обліку. Крім того, може виникнути потреба в перекладі між бездротовими технологіями, протоколами і схемами адресації, а Єдиний реєстр полегшує таку конвертацію. Через численні регуляторні, практичні та безпекові причини, Єдиний реєстр важко впровадити на практиці. Що може бути реалізовано у високорозподілений спосіб, так це логічна сутність, яка вказує на набір даних і атрибутів вузла IoT в мережі «розумного міста».

3.2.4 Система управління ключами

Вузли IoT з обмеженими ресурсами безпечно взаємодіють за допомогою спільного ключа. Симетричні ключі використовуються для простоти та ефективності використання ресурсів.

Управління ключами є критично важливою частиною всіх архітектур безпеки. Ключі повинні генеруватися, зберігатися, передаватися і використовуватися безпечним способом. Розподіл ключів є критичною проблемою для симетричних ключів у розподіленій мобільній системі. Використання ієрархічної системи управління ключами дозволяє ефективно розподіляти ключі, забезпечуючи при цьому безпечне використання симетричних ключів авторизованими пристроями.

Запропонуємо незалежну ієрархічну систему управління та розподілу ключів для кожного рівня протоколу зв'язку. Враховуючи різноманітність функцій, технологій доступу, протоколів та типів вузлів, розумні міста потребують безпечної системи управління ключами для генерації, розподілу, зберігання, відкликання, зміни та використання ключів.

3.3 Протоколи для застосунків «розумного міста»

На рисунку 3.3 показано запропоновану таксономію мережевих протоколів та архітектур для застосунків «розумного міста» (ЗРМ). Він також показує проблеми в комунікаціях IoT через TCP/IP.

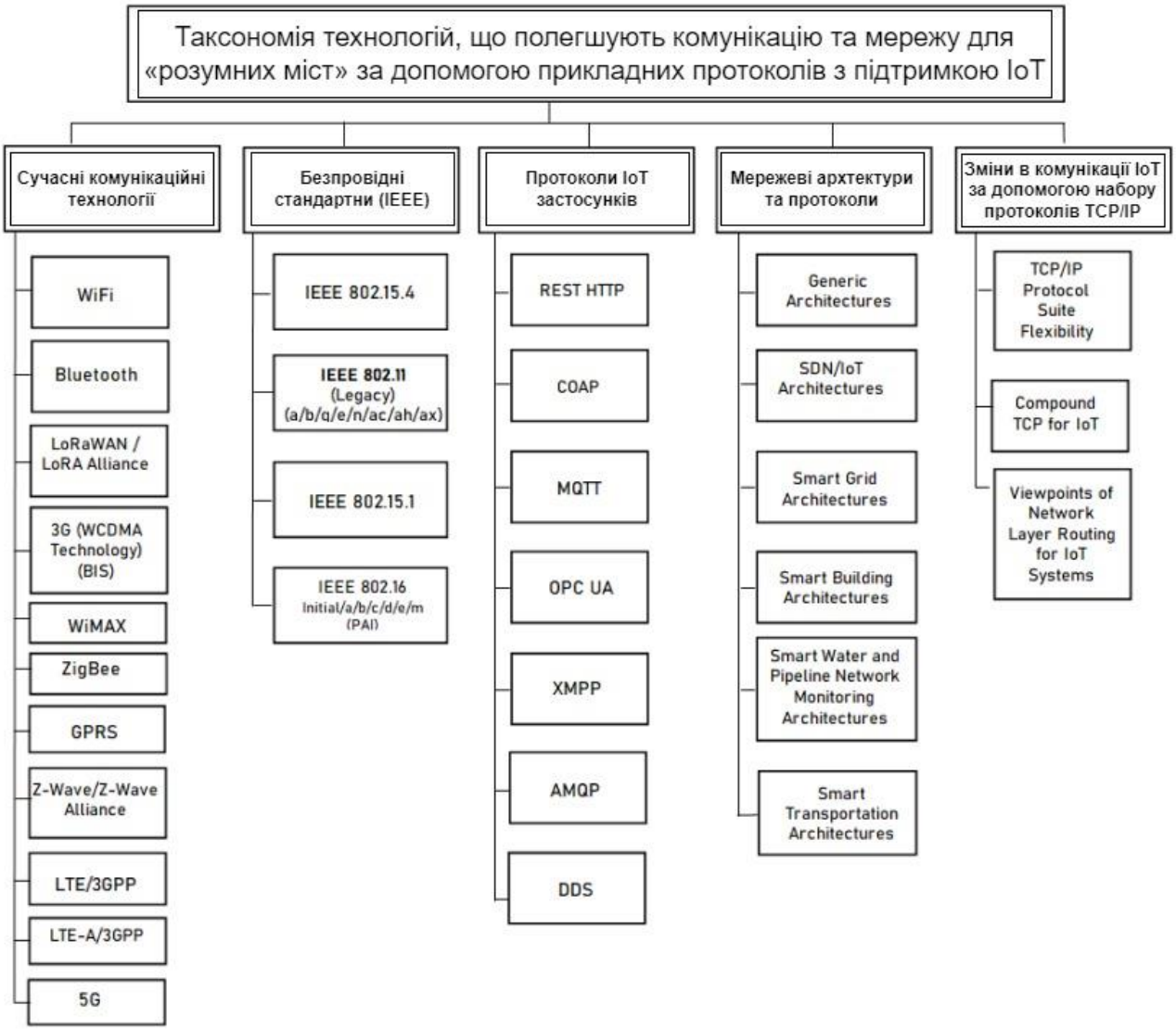

Рисунок 3.3 – Таксономія технологій, що полегшують комунікацію та мережу для «розумних міст» за допомогою прикладних протоколів з підтримкою IoT, а також запропоновані мережеві архітектури та протоколи.

ЗРМ включають численні розумні речі, які працюють на малопотужних акумуляторних пристроях [54]. Нові рішення для підключення досліджуються в світлі наступного питання: чи дозволяють наявні на сьогодні методи,

інструменти та технології - особливо для бездротових мереж - надійно працювати з такою великою кількістю розумних пристроїв?

В роботі [55] надано детальну інформацію про сучасні рішення для підключення, засновані на технологіях WPAN, таких як ZigBee, WiFi, Bluetooth та інших, які пропонують малопотужний D2D-зв'язок. У цих технологіях пропускна здатність, кількість підключених пристроїв, діапазони передачі і т.д. суворо обмежені. Інші технології (наприклад, WiMAX, LTE і LTE-A) передбачають значне енергоспоживання і лише частково застосовні до таких умов. IEEE і 3GPP адаптують свої технології і комунікаційні стратегії до швидко зростаючої перспективи сучасного зв'язку на основі Інтернету речей. Стандарт IEEE 802.11 (WiFi) спочатку був розроблений для забезпечення високої пропускної здатності для меншої кількості станцій, розподілених на меншій відстані в умовах інтер'єру. Через обмеження свого початкового дизайну цей стандарт не підтримує застосунки Інтернету речей. Тому, щоб зробити IEEE 802.11 адаптивним до таких умов, спільнота (IEEE 802.11ah Task Group (TGah)) розробила новий енергоефективний протокол [56]. Вони мають на меті створити систему, яка забезпечить ефективний зв'язок між кількома внутрішніми та зовнішніми пристроями. Тим не менш, реалізація IEEE 802.11ah в реальному часі може потребувати вдосконалення через відсутність відповідного механізму протидії перешкодам.

IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (Zigbee), IEEE 802.11 a/b/g/n, стільниковий зв'язок 3G/4G/5G/LTE/LTE-A і IEEE 802.16 (WiMAX) - це лише кілька прикладів стандартів і протоколів, які слід оцінити на предмет їх придатності для різних ЗРМ. Системи автоматизації «розумного будинку», «розумних будівель» і «розумного сміття» вимагають можливості зв'язку на короткі відстані і можуть використовувати протоколи (наприклад, Bluetooth і Zigbee) з групи WPAN. Ці протоколи відрізняються меншими вимогами до пропускної здатності, мінімальним енергоспоживанням і середовищем комунікаційної інфраструктури з меншим радіусом дії. На противагу цьому, групи локальних мереж, такі як WiFi, можуть використовуватися для ЗРМ, які

потребують зв'язку на більшій відстані. Такими застосунками є інтелектуальні системи управління транспортом.

Протоколи груп WAN, таких як стільниковий зв'язок і WiMAX, можуть бути прийняті застосунками, які потребують зв'язку на великі відстані, такими як інтелектуальні системи реагування на надзвичайні ситуації, системи моніторингу погоди і якості повітря, а також інтелектуальні електромережеві системи. Ці функції, розроблені з точки зору стандартів або протоколів, мають достатньо можливостей, які дозволяють здійснювати як синхронні, так і асинхронні з'єднання для передачі даних. Трафік з максимальними зусиллями (який може ефективно переносити затримки) дозволяє пов'язати функцію асинхронного з'єднання з послугами або застосунками «розумного міста». У той же час, дослідження синхронних з'єднань можливе для тих служб або застосунків, які генерують трафік, що вимагає суворих стандартів QoS, таких як низька затримка і висока доступна пропускна спроможність мережі [57]. Оскільки IEEE 802.15.4 (Zigbee) - це протокол зв'язку малого радіусу дії (з низькою швидкістю передачі даних), який часто передбачає більшу гнучкість для невеликих пристроїв, що працюють на низькому енергоспоживанні, такий протокол може значно збільшити термін служби мережі. Крім того, такий протокол заохочує і вказує на підтримку застосунків і сервісів з відносно м'якими умовами затримки і пропускної здатності в WPAN. Автори роботи [58] використовували WSN на основі IEEE 802.15.4 і запропонували інтелектуальну систему для застосунків освітлення. Автори підкреслили переваги використання бездротових емульсій: нескладність у впровадженні та розгортанні, відносно легке розширення мережі та гнучкість системи завдяки використанню бездротової технології, яка підтримує використання гетерогенних пристроїв в одній і тій же впровадженій та розгорнутій структурі. Крім того, вони підкреслили переваги використання однієї і тієї ж інтелектуальної інфраструктури для різних послуг, що призводить до більш ефективного управління, моніторингу та економічної ефективності. Наприклад, включивши певні інтелектуальні прилади обліку, такі як лічильники води або газу, інтелектуальну мережу або інфраструктуру (яка спочатку була створена для

інтелектуального освітлення) можна також використовувати для інтелектуального обліку.

5G витісняє 4G завдяки вдосконаленим схемам доступу, які називаються множинним доступом BDMA і FBMC, що були вперше запущені в 2015 році. У випадку множинного доступу BDMA часто використовується ортогональний промінь, що означає, що ресурси можуть розподілятися паралельно для кожної мобільної базової станції шляхом поділу променя антени відповідно до положення мобільних станцій, щоб забезпечити множинний доступ до базових станцій. Послідовно це сприяє підвищенню пропускної здатності мереж 5G. Зокрема, ідея переходу до 5G ґрунтується на сучасних технологічних досягненнях і, зокрема, на унікальних потребах клієнтів. Тим не менш, зазвичай вважається, що впроваджені стільникові мережі 5G повинні вирішити значні ускладнення, які не були успішно вирішені в мережах 4G, тобто підвищити пропускну здатність мережі і швидкість передачі даних, зменшити наскрізну затримку (E2E), знизити вартість і забезпечити стабільну якість обслуговування користувачів. Крім того, масове і швидке зростання кількості високорозвинених підключених пристроїв призводить до різкого збільшення мережевого трафіку і розширення спектру застосунків з унікальними динамічними вимогами і можливостями. Досліджуються численні фасилітатори, такі як вибір або використання спектру, масове MIMO, політики управління трафіком і живленням, розвантаження (локальне), а також самоконфігурація і організація мереж, які можуть ефективно вирішити ці проблеми. Завдяки 5G управління і нагляд в режимі реального часу в сценаріях «розумного міста» стануть можливими в наші дні. 5G в кінцевому підсумку націлений на деякі мережеві можливості, а саме: наднадійний зв'язок з низькою затримкою (uRLLC), розширений мобільний широкосмуговий зв'язок (eMBB) і масовий зв'язок машинного типу (mMTC). У контексті «розумного міста» eMBB контролює передачу даних між різноманітними кінцевими пристроями користувачів мережі, периферійними пристроями або хмарними серверами. І навпаки, mMTC спрямована на управління величезними підключеними складними пристроями, такими як носимі пристрої, приводи і давачі, через щільне міське розгортання.

Нарешті, uRLLC бере на себе відповідальність за управління критично важливими до часу комунікаціями, такими як зв'язок між транспортними засобами, базовими станціями і периферійними пристроями [59]. Хоча 5G повністю здійснив нову революцію в галузі мережевих технологій, в цих випадках зв'язку, коли 5G розгортається в контексті «розумних» міст, все ще можливі численні невідомі виклики. Однією з головних проблем є енергоефективний зв'язок, особливо при зв'язку з малопотужними пристроями з акумуляторами, такими як давачі та інші розумні, складні пристрої, що носяться. Крім того, коли дві різні технології (4G/5G) працюють разом, можуть виникнути проблеми. Конкретні проблеми сумісності на рівні пристроїв можуть зберігатися завжди, коли комунікаційна інфраструктура переходить на платформи наступного покоління. Крім того, виникає велике питання, як впоратися з широким розповсюдженням гаджетів, особливо в ізольованих або важкодоступних місцях, а також з потенційними високими витратами, пов'язаними з побудовою і обслуговуванням мереж 5G.

У Додатку А наведено порівняння протоколів, що використовуються для розумних міст.

3.4 Заходи безпеки IoT

IoT передбачає застосування заходів безпеки, використовуючи багато технологій, які будуть розглянуті у цьому підрозділі.

3.4.1 ZigBee

ZigBee: ZigBee розроблений ZigBee Alliance, який є стандартом для персональних мереж (PAN) і є стандартом двостороннього бездротового зв'язку для застосунків малого радіусу дії [60]. ZigBee забезпечує низьку вартість, низьке енергоспоживання, надійний зв'язок. Стек протоколів ZigBee складається з чотирьох рівнів.

ZigBee знаходиться на вершині фізичного рівня і рівня управління доступом до середовища (MAC), які визначені стандартом IEEE 802.15.4. ZigBee

складається з прикладного, мережевого та захисного рівнів. ZigBee взаємодіє безпосередньо з рівнем MAC, який надає наступні послуги [61]:

1. Контроль доступу: MAC вибирає пристрої, з якими потрібно встановити зв'язок, в залежності від MAC-адреси.

2. Шифрування: MAC використовує криптографію з симетричним ключем для захисту даних.

3. Цілісність кадру: Пристрій, який отримує дані, повинен мати можливість виявити модифікацію в повідомленні.

4. Послідовність повідомлень: MAC запобігає атакам повтору, оскільки MAC-кадр використовує структуровані серії значень.

Криптографія ZigBee використовує 128-бітові ключі та шифрування Advanced Encryption Standard (AES) [14]. Використовуються три типи ключів:

1. Мережевий ключ: Використовується у всіх вузлах і є спільним для всіх вузлів мережі ZigBee.

2. Ключ зв'язку: Секретний ключ сеансу для зв'язку між підключеними пристроями.

3. Майстер-ключ: Використовується для генерації ключа зв'язку.

3.4.2 Bluetooth

Bluetooth встановлює бездротові PAN і є відкритим стандартом для радіочастотного зв'язку на коротких відстанях [62]. Існує чотири режими безпеки в Bluetooth:

1. Режим безпеки 1: У цьому режимі процедури безпеки ніколи не ініціюються.

2. Режим безпеки 2: У цьому режимі вводиться авторизація.

3. Режим безпеки 3: Автентифікація та шифрування ввімкнені для всіх з'єднань.

4. Режим безпеки 4: У цьому режимі процедури безпеки ініціюються після встановлення з'єднання.

Крім режимів безпеки, Bluetooth також надає три режими шифрування для забезпечення конфіденційності:

1. Режим шифрування 1: Зв'язок не шифрується.

2. Режим шифрування 2: Індивідуально адресований трафік шифрується.

3. Режим шифрування 3: шифрується весь трафік.

Технологія Bluetooth схильна до мережевих загроз.

Блюджекінг: Полягає в тому, що користувачі надсилають короткі повідомлення (SMS) на інші Bluetooth-пристрої. При цьому зловмисник може бути збережений як контакт, якщо вміст повідомлення не задокументовано належним чином. Таким чином, зловмисник може надсилати будь-який вміст, який буде автоматично відкриватися як такий, що надійшов від відомого контакту.

Автомобільний шептун: У цьому випадку зловмисник може передавати контент на динаміки автомобіля або отримувати контент з мікрофона в автомобілі.

Блюснарфінг: Хакери отримують доступ до Bluetooth-пристроїв і отримують вміст пристроїв через міжнародний ідентифікатор мобільного обладнання (IMEI).

3.4.3 RFID

Автоматична ідентифікація речей і людей здійснюється за допомогою RFID. RFID складається з трьох компонентів: мітки, зчитувача та внутрішньої бази даних [63]. RFID працює в трьох частотних діапазонах: низькочастотному (LF), високочастотному (HF) і надвисокочастотному (UHF). Пристрої RFID поділяються на дві групи.

1. Активні: Активна RFID потребує джерела живлення.

2. Пасивні: Пасивні RFID не потребують батарейок.

Рівні шифрування RFID: Режим шифрування 1: трафік не шифрується, Режим шифрування 2: Стандарт шифрування даних (DES) і Режим шифрування 3: AES-128 біт.

Незважаючи на вищезгадані режими шифрування, RFID має потенційні загрози безпеці, які обговорюються нижче:

1. Несанкціоноване сканування - у цьому випадку RFID-мітки скануються без дозволу.

2. Таємне відстеження - ідентифікатор чіпа опускається без будь-якої інформації про власника мітки.

3. Скімінг і клонування - копіювання мітки можливе, якщо секрети мітки відомі хакеру.

4. Криптографічні вразливості - зашифровані дані можуть бути розшифровані, якщо застосовано слабке шифрування.

3.4.4 WiFi

WiFi забезпечує бездротовий зв'язок і надає доступ до Інтернету у вигляді радіосигналів [64]. Можливі атаки можуть бути спрямовані на контроль доступу до мережі, безпеку даних та дизайн мережі [65]. WiFi використовує шість режимів безпеки:

1. Режим безпеки 1: Загальна безпека мережевої інформації WiFi.

2. Режим безпеки 2: Дротовий еквівалент конфіденційності (WEP), захищений доступ WiFi (WPA) і шифрування WPA2.

3. Режим безпеки 3: фільтрація MAC-адрес.

4. Режим безпеки 4: Фільтрація протоколів.

5. Режим безпеки 5: Екран ідентифікатора набору послуг (SSID) широкомовної інформації.

6. Режим безпеки 6: Присвоєння IP-адреси.

WiFi також вразливий до багатьох загроз, а саме: підслуховування бездротової мережі: Інформація збирається з мережі шляхом підглядання переданих даних та атака на пошуковий бездротовий сигнал: Коли пристрій шукає бездротову мережу, і якщо мережа не зашифрована, підключення до такої мережі є потенційно небезпечним.

3.5 Висновок до третього розділу

У цьому розділі було розглянуто основні компоненти безпечної архітектури Інтернету речей (IoT) для розумного міста. Основні компоненти включають чорні мережі для захисту даних і забезпечення конфіденційності, довірені контролери SDN для безпечної маршрутизації, єдиний реєстр для управління ідентифікацією пристроїв та систему управління ключами для забезпечення безпеки комунікацій.

Чорні мережі забезпечують конфіденційність, цілісність і приватність даних, шифруючи як корисне навантаження, так і метадані. Довірені контролери SDN вирішують проблеми маршрутизації в чорних мережах, забезпечуючи синхронізацію вузлів і динамічне прокладання маршрутів. Єдиний реєстр консолідує різні технології, схеми адресації і типи пристроїв, спрощуючи управління ідентифікацією та аутентифікацією. Система управління ключами відповідає за безпечне генерацію, зберігання, розподіл та використання ключів у мережах IoT, що дозволяє ефективно захищати комунікації між пристроями.

У підсумку, запропонована архітектура забезпечує комплексний підхід до безпеки IoT у розумних містах, вирішуючи проблеми конфіденційності, автентифікації, авторизації і управління ключами. Це дозволяє створити надійні та безпечні IoT-системи, які можуть ефективно функціонувати у складних і гетерогенних середовищах розумного міста.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Питання щодо охорони праці

Тема кваліфікаційної роботи освітнього рівня «Магістр» присвячена мережевим архітектурам та протоколам Інтернету речей у «розумних містах». Тому доцільно розглянути питання вдосконалення охорони праці в ІТ.

На перший погляд, робота за комп'ютером здається безпечною, але саме легковажність до неї може призвести до певних проблем у здоров'ї людини. Професія програміста та інших фахівців ІТ-технологій пов'язана з колосальним розумовим напруженням. Розробники – настільки захоплені люди, що навіть відволікаючись від роботи над проєктом, продовжують думати про роботу. Нерідко відпочинком вони вважають паралельну заміну основної діяльності, наприклад, читання профільної літератури, верстку сайтів, вивчення нових мов програмування. Однак мозок не може до безкінечності приймати виключно корисну інформацію, яку розробник прагне направляти в русло особистісного та професійного зростання.

Зараз багато ІТ-компаній обладнують свої офіси кімнатами відпочинку та лаунж-зонами, які забезпечують психофізіологічне розвантаження працівників. Адже окремим робочим столом з ноутбуком вже давно нікого не здивуєш. Тому, бажаючи підвищити продуктивність працівників, міжнародні компанії змагаються, перетворюючи нудні одноманітні офіси в креативні простори, де нові ідеї народжуються без титанічних зусиль.

При цьому не варто забувати, що умови праці програмістів також характеризуються можливістю впливу на них наступних небезпечних і шкідливих виробничих факторів: шуму; тепловиділень, причому шкоди організму можуть завдати не тільки високі, але і низькі температури; іонізуючих і неіонізуючих випромінювань: рентгенівське, інфрачервоне, електромагнітне випромінювання ВЧ і СВЧ діапазону; статичної електрики; недостатнє штучне та природнє освітлення; візуальні фактори: яскравість, контрастність, мерехтіння зображення, відблиски тощо.

За таких умов зростає роль та значення охорони праці, як системи правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. Адже в кінцевому рахунку плоди науково-технічного прогресу можуть бути ефективними лише в тій мірі, в якій вони забезпечують людині безпеку, комфортність і зручність трудової діяльності.

Таким чином, використання новітніх інформаційно-комунікаційних технологій вимагає від фахівців ІТ-індустрії додержання певних правил та вимог з точки зору безпеки праці, її нормування з урахуванням віку працюючих та загального інформаційного навантаження, розробки та впровадження індивідуальних, щотижневих та щорічних режимів праці та відпочинку, які сприятимуть профілактиці перевтомлення і підвищенню розумової працездатності працюючих. Особливу роль в цьому напрямі повинні відігравати ергономічні заходи стосовно створення робочих місць, оптимізації взаємодії людини в рамках системи «оператор-термінал». Всі ці вимоги повинні бути втілені у відповідних нормативно-правових актах (стандартах підприємств), що регламентують різноманітні питання охорони та психології безпеки праці фахівців ІТ-індустрії/

Поява та впровадження нових інформаційно-комунікаційних технологій зумовлює необхідність подальшого вдосконалення охорони праці фахівців ІТ-індустрії.

З метою належного правового забезпечення необхідно розширити ти доповнити перелік основних професій комп’ютерної галузі у національному класифікаторі ДК-003-2010, а також підготувати відповідний випуск у кваліфікаційному довіднику посад фахівців ІТ-індустрії, що сприятиме вирішенню питань їх соціального захисту, пенсійного забезпечення, атестації робочих місць основних професій за умовами праці на предмет подальших певних видів пільг та компенсацій за важкі шкідливі і небезпечні умови праці.

Важливим напрямом стосовно визначення професійної придатності фахівців з інформаційних технологій є проведення психофізіологічної експертизи відповідно до 5 статті Закону України «Про охорону праці».

Робота з комп'ютерами нового покоління характеризується певним психофізіологічними перенавантаженнями, втомою зорового аналізатора, гіпокінезією, відсутність диференційованих норм праці при роботі з новою комп'ютерною технікою в залежності від віку, статі, категорії зорової роботи, режимів праці і відпочинку (протягом робочого дня, тижня, щорічного режиму відпусток).

Все це потребує розробки нових нормативно-правових актів з регламентації праці та відпочинку фахівців ІТ-індустрії і стандартів підприємств, центрів комп'ютерної техніки, центрів інформаційних технологій, сучасних комп'ютерних класів.

Особлива роль з точки зору збереження та відновлення здоров'я працюючих в комп'ютерні' галузі належить попереднім та періодичним наглядам з подальшої психофізіологічної експертизи і встановленням професійної придатності при роботі з комп'ютерами нового покоління, який супроводжується виникненням певних факторів професійного ризику електротравматизму при їх ремонті та обслуговуванні. В цьому зв'язку необхідне запровадження експертизи на предмет безпечної експлуатації ПЕОМ, тобто офіційне підтвердження фактичних параметрів електробезпеки, їх відповідності вимогам нормативної документації фахівців, які проводять таку експертизу повинні пройти навчання і перевірку знань відповідно до вимог ДНАОП 0.00-8.20-99. За результатами експертизи повинні прийматися рішення про відповідність ПЕОМ нормам безпеки, терміни чергової експертизи, оформлюються протоколи вимірювань і випробувань, проведені у разі потреби розрахунки та експертний висновок [66].

Для підвищення розумової працездатності то зорової роботи повинна здійснюватися ергономічна оптимізація в рамках системи «оператор-термінал», яка сприятиме результативній фізичній та інтелектуальний працездатності і відновленню психосоматичного здоров'я фахівців ІТ-індустрії.

4.2 Питання щодо безпеки в надзвичайних ситуаціях

Тема кваліфікаційної роботи освітнього рівня «Магістр» присвячена використанням захищених мережевих архітектур та протоколів Інтернету речей. Тому доцільно розглянути питання охорони праці користувачів ПК.

Широке розповсюдження отримали персональні комп'ютери. Однак їх використання загострило проблеми збереження власного та суспільного здоров'я, вимагає удосконалення існуючих та розробки нових підходів до організації робочих місць, проведення профілактичних заходів для запобігання розвитку негативних наслідків впливу ПК на здоров'я користувачів.

Заходи з охорони праці користувачів ПК необхідно розглядати в трьох основних аспектах: соціальному, психологічному та медичному.

У соціальному плані розв'язання цих проблем пов'язане з опти-мізацією умов життя, праці, відпочинку, харчування, побуту, розвитком культури, транспорту.

Значне місце у профілактиці розладів здоров'я належить психології праці. Тому заходи, пов'язані з формуванням раціональних виробничих колективів, у яких відсутня психологічна несумісність, сприяють зменшенню нервово-психічного перенапруження, підвищенню працездатності та ефективності праці.

Особливої значущості у користувачів відеодисплейних терміналів набуває психоемоційний стрес, який більшою або меншою мірою проявляється у кожного з них.

Оскільки цю проблему відразу вирішити неможливо, доцільно на рівні підприємства, організації послідовно усувати такі виробничі умови, які є сприятливими для розвитку емоційного стресу.

Значна роль у профілактиці захворювань користувачів ПК відводиться медицині. Існує перелік профілактичних заходів для користувачів ПК, що включає як складові первинної профілактики здоров'я (професійний відбір), так і вторинної, яка направлена на зниження ймовірності розвитку перевтоми та

перенапруження. Ці комплексні заходи спрямовані на відновлення функціонального стану зорового та опорно-рухового апарату.

Наказ Мінсоцполітики від 14.02.2018 р. №207 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» (далі – Вимоги), зареєстрований в Міністерстві юстиції України 25 квітня 2018 року №508/31960, поширюється на всіх суб'єктів господарювання незалежно від форм власності, організаційно-правової форми і видів діяльності та встановлюють мінімальні вимоги безпеки та захисту здоров'я під час здійснення роботи, пов'язаної з використанням екранних пристроїв незалежно від їхнього типу та моделі.

Окрім того, відповідно до Закону України «Про охорону праці» роботодавець зобов'язаний:

- поінформувати працівників під розписку про умови праці та наявність на їх робочих місцях небезпечних та шкідливих виробничих факторів (фізичних, хімічних, біологічних, психофізіологічних), які виникають під час роботи з екранними пристроями та ще не усунуто, а також про можливі наслідки їх впливу на здоров'я працівників.
- забезпечити навчання і перевірку знань працівників з питань охорони праці та безпечного використання екранних пристроїв до початку роботи з ними, а також у випадках модифікації та організації роботи обладнання.
- роботодавець повинен вжити відповідних заходів, щоб забезпечити відповідність робочого місця працівника до цих Вимог.
- під час облаштування робочого місця працівника з екранними пристроями необхідно обирати таке устаткування, яке не створює зайвого шуму та не виділяє надлишкового тепла. Рівні шуму на робочих місцях осіб, які працюють з екранними пристроями, мають відповідати вимогам Санітарних норм виробничого шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99, затверджених постановою Головного державного санітарного лікаря України від 01.12.1999 р. №37.
- повинен за рахунок тривалості робочої зміни організувати внутрішні регламентовані перерви для відпочинку відповідно до Державних санітарних

правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98, затверджених постановою Головного державного санітарного лікаря України від 10.12.1998 р. №7 (далі – ДСанПІН 3.3.2.007-98).

- забезпечити за свій рахунок проведення медичних оглядів працівників відповідно до вимог Порядку проведення медичних оглядів працівників певних категорій, затвердженого наказом МОЗ від 21.05.2007 р. №246, зареєстрованого в Міністерстві юстиції України 23 липня 2007 року за №846/14113.
- роботодавець зобов'язаний за необхідності проводити лабораторні дослідження умов праці працівників з метою виявлення шкідливих і небезпечних факторів виробничого середовища, важкості та напруженості трудового процесу (зокрема щодо виявлення ризиків, пов'язаних із погіршенням зору, порушенням фізичного стану, стресом) та вживати заходів щодо усунення виявлених ризиків.

Окремо зазначаємо, що за характером трудової діяльності при роботі з відеотерміналами електронно-обчислювальних машин (далі – ЕОМ) та персональних електронно-обчислювальних машин (далі – ПЕОМ) виділено три професійні групи згідно з діючим класифікатором професій:

- розробники програм (інженери-програмісти) – виконують роботу переважно з відео терміналом (далі – ВДТ) та документацією при необхідності інтенсивного обміну інформацією з ЕОМ і високою частотою прийняття рішень. Робота характеризується інтенсивною розумовою творчою працею з підвищеним. напруженням зору, концентрацією уваги на фоні нервово-емоційного напруження, вимушеною робочою позою, загальною гіподинамією періодичним навантаженням на кисті верхніх кінцівок. Робота виконується в режимі діалогу з ЕОМ у вільному темпі з періодичним пошуком помилок в умовах дефіциту часу;
- оператори електронно-обчислюваних машин – виконують роботу, яка пов'язана з обліком інформації одержаної з ВДТ за попереднім запитом, або тієї, що надходить з нього, супроводжується перервами різної тривалості, пов'язана з виконанням іншої роботи і характеризується як робота з

напруженням зору, невеликими фізичними зусиллями нервовим напруженням середнього ступення та виконується у вільному темпі;

- оператор комп'ютерного набору – виконує одноманітні за характером роботи з документацією та клавіатурою і нечастими нетривалими переключеннями погляду на екран дисплея, з введенням даних з високою швидкістю, робота характеризується як фізична праця з підвищеним навантаженням на кисті верхніх кінцівок на фоні загальної гіподинамії з напруженням зору (фіксація зору переважно на документі), нервово-емоційним напруженням.

Відповідно до наведеної вище класифікації та згідно з вимогами ДСанПІН 3.3.2.007-98 є такі внутрішньозмінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці:

- для розробників програм із застосуванням ЕОМ, слід призначати регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи.
- для операторів із застосуванням ЕОМ, слід призначати регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні дві години роботи;
- для операторів комп'ютерного набору слід призначати регламентовані перерви для відпочинку тривалістю 10 хвилин після кожної години роботи.

При 12-годинній робочій зміні регламентовані перерви повинні встановлюватися в перші 8 годин роботи аналогічно перервам при 8-годинній робочій зміні, а протягом останніх 4-х годин роботи, незалежно від характеру трудової діяльності, через кожну годину тривалістю 15 хвилин.

Отже, встановлені відповідно до вимог ДСанПІН 3.3.2.007-98 внутрішньозмінні режими праці та відпочинку при роботі з електронно-обчислювальними машинами повинні входити в тривалість робочої зміни [66].

4.3 Висновок до четвертого розділу

В третьому розділі кваліфікаційної роботи описано охорону праці користувачів ПК та безпечне поводження з електронними пристроями.

Україна надалі вступає у еру широкого використання комп'ютерів у повсякденному житті, проте процес узгодження норм та умов роботи з цифровою технікою ще не завершено. У порівнянні з іноземними ІТ-компаніями, де цей процес вже укорінився, українські підприємства відстають, але підходять до завершальних етапів адаптації.

Не дивлячись на те, що робота за комп'ютером може здаватися безпечною, увага звертається на легковажність до цього процесу, яка може викликати проблеми у здоров'ї людини. Зокрема, висвітлено, що професія програміста та інших ІТ-фахівців супроводжується великим розумовим напруженням, а відсутність повного відпочинку може призвести до перевтоми та стресу.

У контексті охорони праці відзначено ряд факторів, які можуть впливати на здоров'я працівників ІТ-сфери, включаючи шум, тепловиділення, випромінювання, статичну електрику та освітлення. Підкреслено, що з урахуванням зростаючого значення цифрової техніки в організаціях, важливо розвивати та впроваджувати ефективні стратегії охорони праці для забезпечення безпеки та здоров'я працівників.

Важливу роль у вирішенні цих проблем відіграє психологія праці та медицина. Акцентується, що формування здорових виробничих колективів і психологічний комфорт є ключовими чинниками для зменшення нервово-психічного напруження та підвищення працездатності. Окрім того, наголошується на важливості медичних заходів та профілактичних програм для користувачів комп'ютерів з метою попередження ризиків та забезпечення стабільного функціонального стану зорового та опорно-рухового апарату.

У цілому, здійснено висновок, що із зростанням використання комп'ютерної техніки у різних сферах суспільства, необхідно вдосконалювати стратегії охорони праці, звертаючи увагу на соціальні, психологічні та медичні аспекти для забезпечення здоров'я та безпеки користувачів ПК.

ВИСНОВКИ

Концепція «розумного міста» спрямована на ефективне використання ресурсів, зниження операційних витрат та підвищення якості життя мешканців за допомогою інтеграції різних технологій, включаючи Інтернет речей (IoT), бездротові сенсорні мережі (WSN), кіберфізичні системи (CPS), хмарні обчислення (ClCom), туманні обчислення (FoC), аналітику великих даних і роботів. Виявлено, що для досягнення цих цілей важливу роль відіграє ефективна мережа та комунікація між багатьма компонентами, які забезпечують функціонування різних складових розумного міста.

Дослідження підкреслюють необхідність створення гнучких і керованих мережевих платформ для забезпечення роботи «розумних» мереж, будівель, систем. Визначено ключові мережеві потреби та відповідні протоколи, які можуть бути застосовані на різних рівнях системи. Особлива увага приділена питанням безпеки та конфіденційності, які стають все більш важливими в IoT. Розроблено архітектури з функціями автентифікації, авторизації та контролю доступу, що гарантують безпечний доступ до системних послуг.

Значний прогрес досягнуто у сфері безпеки та конфіденційності IoT, зокрема завдяки криптографічним методам управління ключами та ідентифікацією, а також технологіям забезпечення цілісності даних. Однак, залишається багато відкритих дослідницьких питань, таких як автономні обчислення для безпеки, неспостережувані комунікації для покращення конфіденційності, анонімізація трафіку і побудова довіри між пристроями.

Крім того, безпека на мережевому рівні розумного міста є критично важливою для зменшення та пом'якшення впливу потенційних загроз. Для цього необхідно впровадження системи моніторингу обізнаності та управління ризиками безпеки в реальному часі.

У підсумку розроблено детальний огляд протоколів та архітектур для розумних міст, допомагає виявити прогалини в існуючих дослідженнях та пропонує можливі рішення для покращення безпеки та конфіденційності в

системах IoT, що сприятиме успішному впровадженню розумних міст і підвищенню якості життя їх мешканців.

В першому розділі кваліфікаційної роботи освітнього рівня «Магістр»:

– Розглянуто архітектуру системи Інтернету речей

– Проаналізовано елементи безпеки в «розумних містах»

– Обґрунтовано важливість питань захисту та безпеки для протоколів IoT

В другому розділі кваліфікаційної роботи:

– Описано виклики безпеки та конфіденційності

– Досліджено методології захисту архітектури «розумного міста»

В третьому розділі кваліфікаційної роботи:

– Запропоновано компоненти безпечної архітектури IoT та протоколів в «розумному місті»

У розділі «Охорона праці та безпека в надзвичайних ситуаціях» проаналізовано охорону праці користувачів ПК та безпечне поводження з електронними пристроями.

ПЕРЕЛІК ДЖЕРЕЛ

1 Abid, Muhammad Aneeq, et al. "Evolution towards smart and software-defined internet of things." AI 3.1 (2022): 100-123.

2 Vermesan, Ovidiu, et al. "Internet of things strategic research and innovation agenda." Internet of things. River Publishers, 2022. 7-151.

3 Sankar, SM Udhaya, Mary Subaja Christo, and PS Uma Priyadarsini. "Secure and energy concise route revamp technique in wireless sensor networks." Intelligent Automation and Soft Computing 35.2 (2023): 2337-2351.

4 Menon, Varun G., et al. "An IoT-enabled intelligent automobile system for smart cities." Internet of Things 18 (2022): 100213.

5 Ismagilova, Elvira, et al. "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework." Information Systems Frontiers (2022): 1-22.

6 Sharma, Avani, et al. "Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes." Computer Communications 160 (2020): 475-493.

7 HaddadPajouh, Hamed, et al. "A survey on internet of things security: Requirements, challenges, and solutions." Internet of Things 14 (2021): 100129.

8 Mishra, Nivedita, and Sharnil Pandya. "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review." IEEE Access 9 (2021): 59353-59377.

9 Badr, Youakim, Xiaoyang Zhu, and Mansour Naser Alraja. "Security and privacy in the Internet of Things: threats and challenges." Service Oriented Computing and Applications 15.4 (2021): 257-271.

10 Malhotra, Parushi, et al. "Internet of things: Evolution, concerns and security challenges." Sensors 21.5 (2021): 1809.

11 Peng, Kai, et al. "Security challenges and opportunities for smart contracts in Internet of Things: A survey." IEEE Internet of Things Journal 8.15 (2021): 12004-12020.

12 Omolara, Abiodun Esther, et al. "The internet of things security: A survey encompassing unexplored areas and new insights." Computers & Security 112 (2022): 102494.

13 Syed, Abbas Shah, et al. "IoT in smart cities: A survey of technologies, practices and challenges." Smart Cities 4.2 (2021): 429-475.

14 Sharma, Rohit, and Rajeev Arya. "Security threats and measures in the Internet of Things for smart city infrastructure: A state of art." Transactions on Emerging Telecommunications Technologies 34.11 (2023): e4571.

15 Mansour, Mohammad, et al. "Internet of things: a comprehensive overview on protocols, architectures, technologies, simulation tools, and future directions." Energies 16.8 (2023): 3465.

16 Stergiou, Christos L., Elisavet Bompoli, and Konstantinos E. Psannis. "Security and privacy issues in IoT-based big data cloud systems in a digital twin scenario." Applied Sciences 13.2 (2023): 758.

17 Sarker, Iqbal H., et al. "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions." Mobile Networks and Applications 28.1 (2023): 296-312.

18 Rekha, Shashi, et al. "Study of security issues and solutions in Internet of Things (IoT)." Materials Today: Proceedings 80 (2023): 3554-3559.

19 Ghazal, Taher M., et al. "Machine learning approaches for sustainable cities using internet of things." The Effect of Information Technology on Business and Marketing Intelligence Systems. Cham: Springer International Publishing, 2023. 1969-1986.

20 Rao, P. Muralidhara, and Bakkiam David Deebak. "Security and privacy issues in smart cities/industries: technologies, applications, and challenges." Journal of Ambient Intelligence and Humanized Computing 14.8 (2023): 10517-10553.

21 Al-Turjman, Fadi, Hadi Zahmatkesh, and Ramiz Shahroze. "An overview of security and privacy in smart cities' IoT communications." Transactions on Emerging Telecommunications Technologies 33.3 (2022): e3677.

22 Haque, AKM Bahalul, Bharat Bhushan, and Gaurav Dhiman. "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends." Expert Systems 39.5 (2022): e12753.

23 Vermesan, Ovidiu, et al. "Internet of things beyond the hype: Research, innovation and deployment." Building the Hyperconnected Society-Internet of Things Research and Innovation Value Chains, Ecosystems and Markets. River Publishers, 2022. 15-118.

24 Vasile, Mazilescu. "IoT as a Central Disruptive Technology in the Development of Hyperconnected Business and Social Models." Risk in Contemporary Economy (2021): 261-275.

25 Siwakoti, Yuba Raj, et al. "Advances in IOT security: Vulnerabilities, enabled Criminal Services, attacks and countermeasures." IEEE Internet of Things Journal (2023).

26 Jofre, Marc, et al. "Cybersecurity and privacy risk assessment of point-of-care systems in healthcare—a use case approach." Applied Sciences 11.15 (2021): 6699.

27 Ungurean, Ioan, and Nicoleta Cristina Gaitan. "A software architecture for the Industrial Internet of Things—A conceptual model." Sensors 20.19 (2020): 5603.

28 Zhao, Liqing, Bo Cheng, and Junliang Chen. "Service-oriented IoT resources access and provisioning framework for IoT context-aware environment." 2020 IEEE World Congress on Services (SERVICES). IEEE, 2020.

29 Benotmane, Meryem, Kaoutar Elhari, and Adil Kabbaj. "Survey of IoT Reference Architectures and Models and IoT Initiatives." Proceedings of the Future Technologies Conference (FTC) 2021, Volume 1. Springer International Publishing, 2022.

30 Fabrègue, Brian FG, and Andrea Bogoni. "Privacy and security concerns in the smart city." Smart Cities 6.1 (2023): 586-613.

31 Spirito, Maurizio, et al. "Internet of Things Applications-From Research and Innovation to Market Deployment." Internet of Things Applications-From Research and Innovation to Market Deployment. River Publishers, 2022. 243-285.

32 Baldini, Gianmarco, et al. "Internet of things privacy, security and governance." Internet of Things. River Publishers, 2022. 207-224.

33 Kh, Teeba, and Ibrahim Hamarash. "Model-based quality assessment of internet of things software applications: A systematic mapping study." (2020): 128-152.

34 Denti, Enrico. "Novel pervasive scenarios for home management: the Butlers architecture." SpringerPlus 3 (2014): 1-30.

35 Mahalle, Parikshit N., Gitanjali Rahul Shinde, and Arvind Vinayak Deshpande. The convergence of internet of things and cloud for smart computing. CRC Press, 2021.

36 Baldini, Gianmarco, et al. "Internet of things privacy, security and governance." Internet of Things. River Publishers, 2022. 207-224.

37 Kolarić, Siniša, and Dennis Shelden. "Toward an open IoT implementation for urban environments: The architecture of the DBL SmartCity platform." Smart Cities and Smart Governance: Towards the 22nd Century Sustainable City (2021): 345-372.

38 Camatti, Juliane Andressa, et al. "Comparative study of open IoT architectures with TOGAF for industry implementation." Procedia Manufacturing 51 (2020): 1132-1137.

39 Bhattacharjya, Aniruddha, et al. "Present scenarios of IoT projects with security aspects focused." Digital Twin Technologies and Smart Cities (2020): 95-122.

40 Spirito, Maurizio A., and Maria T. Delgado. "Internet of Things application scenarios, pilots and innovation." Building the Hyperconnected Society-Internet of Things Research and Innovation Value Chains, Ecosystems and Markets. River Publishers, 2022. 119-144.

41 bCEA, L. I. S. T. "USEIT Project: Empowering the Users to Protect Their Data." Security and Privacy in the Internet of Things: Challenges and Solutions 27 (2020): 1.

42 Das, Sangjukta, and Suyel Namasudra. "Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure." IEEE Transactions on Industrial Informatics 19.1 (2022): 821-829.

43 Pitu L et al (eds) (2015) End-to-End Security and Privacy: Design and Open Specification COSMOS Project Deliverable D3.1.2, 30 April 2015

44 van Oorschot, Paul C. "Public Key Cryptography’s Impact on Society: How Diffie and Hellman Changed the World." Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman. 2022. 19-56.

45 Schreckling D et al (2015) The Compose Security Framework, COMPOSE Deliverable D5.4.2, 15 Nov 2015

46 Li, Peixuan, and Danfeng Zhang. "Towards a general-purpose dynamic information flow policy." 2022 IEEE 35th Computer Security Foundations Symposium (CSF). IEEE, 2022.

47 Koo, Jahoon, and Young-Gab Kim. "Resource identifier interoperability among heterogeneous IoT platforms." Journal of King Saud University-Computer and Information Sciences 34.7 (2022): 4191-4208.

48 Hussain, Mohamed Fazil, et al. "Analyzing Application Response Time Lag: in Mobile Edge and Fog Computing Environments." 2023 Eighth International Conference on Fog and Mobile Edge Computing (FMEC). IEEE, 2023.

49 Lorünser T, Länger T, Slamanig D, Pöhls HC (2016) PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services. In: Proceedings of a workshop on security, privacy, and identity management in the cloud collocated at the 11th international conference on availability, reliability and security. ARES’16, Salzburg, Austria, 2016

50 Ghazal, Taher M., et al. "Internet of things connected wireless sensor networks for smart cities." The Effect of Information Technology on Business and Marketing Intelligence Systems. Cham: Springer International Publishing, 2023. 1953-1968.

51 Kabir, Sohag, Prosanta Gope, and Saraju P. Mohanty. "A security-enabled safety assurance framework for iot-based smart homes." IEEE Transactions on Industry Applications 59.1 (2022): 6-14.

52 Basharat, Asma, and Mohd Murtadha Bin Mohamad. "Security challenges and solutions for internet of things based smart agriculture: A review." 2022 4th International Conference on Smart Sensors and Application (ICSSA). IEEE, 2022.

53 Alam, Iqbal, et al. "A survey of network virtualization techniques for Internet of Things using SDN and NFV." ACM Computing Surveys (CSUR) 53.2 (2020): 1-40.

54 Syed, A.S.; Sierra-Sosa, D.; Kumar, A.; Elmaghraby, A. IoT in smart cities: A survey of technologies, practices and challenges. Smart Cities 2021, 4, 429–475.

55 Ahad, Mohd Abdul, et al. "Enabling technologies and sustainable smart cities." Sustainable cities and society 61 (2020): 102301.

56 De Koninck, Tobia, et al. "Experimental validation of IEEE 802.11 ah propagation models in heterogeneous smarty city environments." GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020.

57 Mamatas, Lefteris, et al. "Protocol-adaptive strategies for wireless mesh smart city networks." IEEE Network 37.2 (2023): 136-143.

58 Bouzid, S. E., et al. "Wireless sensor and actuator network deployment optimization for a lighting control." International Journal of Computer and Communication Engineering 9.2 (2020): 15.

59 Yang, Chen, et al. "Using 5G in smart cities: A systematic mapping study." Intelligent Systems with Applications 14 (2022): 200065.

60 Zohourian, Alireza, et al. "IoT Zigbee device security: A comprehensive review." Internet of Things (2023): 100791.

61 Adi, Puput Dani Prasetyo, et al. "A performance evaluation of ZigBee mesh communication on the Internet of Things (IoT)." 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT). IEEE, 2021.

62 Lacava, Andrea, et al. "Securing Bluetooth Low Energy networking: An overview of security procedures and threats." Computer Networks 211 (2022): 108953.

63 Costa, Filippo, et al. "A review of RFID sensors, the new frontier of internet of things." Sensors 21.9 (2021): 3138.

64 Taneja, Ashu, et al. "An improved WiFi sensing based indoor navigation with reconfigurable intelligent surfaces for 6G enabled IoT network and AI explainable use case." Future Generation Computer Systems 149 (2023): 294-303.

65 Aziz, Azlan Abd, and Syamsuri Yaacob. "IoT Performance and Security Analysis Based on WiFi Systems." Proceedings of the Multimedia University Engineering Conference (MECON 2022). Vol. 214. Springer Nature, 2023.

66 Стручок В.С. Безпека в надзвичайних ситуаціях. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання / В.С.Стручок. — Тернопіль: ФОП Паляниця В. А., 2022. — 156 с

67 Stanko, A., Palka, O., Matiichuk, L., Martsenko, N., & Matsiuk, O. (2021, September). Smart City: A Review of Model Architecture and Technology. In 2021 IEEE 16th International Conference on Computer Sciences and Information Technologies (CSIT) (Vol. 2, pp. 273-277). IEEE.

68 Palka, O., Kunanets, N., Pasichnyk, V., Matsiuk, O., & Matsiuk, S. (2023). Comparative Analysis of Smart City Platforms. In COLINS (3) (pp. 487-499).

ДОДАТКИ

Додаток А

Порівняння протоколів, що використовуються для розумних міст.

Комунікаційні технології/стандарти	Робочі діапазони частот	Модуляція даних і чутливість приймача	Специфікації канального рівня	Швидкість передачі даних	Територія покриття
ZigBee/IEEE 802.15.4	2.4 ГГц, 868 МГц–915 МГц (DSSS)	**Модуляція даних**: 16-арна ортогональна модуляція (2,4 ГГц) і BPSK з DE (868 МГц-915 МГц). **Чутливість приймача:** -85 дБм (2,4 ГГц PHY) -92 дБм (868/915 МГц PHY)	CSMA-CA, TDD (optional)	250 Kbps (2.4 ГГц), 20 Kbps (868 МГц), and 40 Kbps (915 МГц)	30–50 м
Bluetooth/ IEEE 802.15.1	2.4 ГГц, 2400 МГц–2483.5 МГц (FHSS/FSK)	**Модуляція даних:** GFSK і PSK (для більш високих швидкостей передачі даних) - π/4 DQPSK і 8 DPSK **Чутливість приймача:** від -70 дБм до -82 дБм (зазвичай залежить від типу використання PHY), наприклад, Bluetooth LE 125K (Coded) PHY може досягати -103 дБм	TDD, M&S, FH	1 Mbps	1–100 м
WiFi/IEEE 802.11 (Legacy) (a/b/g/n)	Conventional: 2.4 ГГц a: 5 ГГц (OFDM), b: 2.4 ГГц (DSSS), g: 2.4 ГГц (DSSS, OFDM), n: 5 ГГц (DSSS, OFDM)	**Модуляція даних:** Звичайна: DI, DSSS і FHSS, a: OFDM b: HR-DSSS, g: OFDM, DSSS і CCK n: OFDM з використанням MIMO та CB **Чутливість приймача:** Застаріла: 1 Мбіт/с: -80 дБм, 2 Мбіт/с: -75 дБм b: 2 Мбіт/с: -80 дБм, 11 Мбіт/с -76 дБм g: 6-54 Мбіт/с: від -82 дБм до -65 дБм n: 1-54 Мбіт/с: від -80 дБм до -65 дБм	CSMA-CA	Conventional: 1–2 Mbps a: 6–54 Mbps (VMT) b: 1–11 Mbps (VMT) g: 6–54 Mbps (VMT) n: 1–54 Mbps (VMT)	1–100 м
WiMAX/IEEE 802.16	2.5 ГГц, 3.5 ГГц, 5.8 ГГц (MIMO-OFDM)	**Модуляція даних:** OFDM з використанням MIMO, AMC, AAS **Чутливість приймача:** QPSK (1/2): -80 дБм, QPSK (3/4): -78 дБм 16 QAM (1/2): -73 дБм, 16 QAM (3/4): -71 дБм 64 QAM (2/3): -66 дБм, 64 QAM (3/4): -65 дБм	TDD, FDD	75 Mbps	1–5 км (NLoS), 10–50 км (LoS)
LoRaWAN/LoRA Alliance	867–869 МГц (Europe) 865–867 МГц (India)	**Модуляція даних:** LoRA (CSSM) **Чутливість приймача:** -137 дБм (SF = 12, BW = 125 КГц, NF = 6)	Pure ALOHA with DCLs or PSA (LBT)	250 bps–50 Kbps (Europe) NS (India)	2–5 км
3G (WCDMA Technology) (BIS)	1.92–1.98 ГГц, 2.11–2.17 ГГц (licensed)	**Модуляція даних**: AM/PSK з використанням QAM **Чутливість приймача**: -102 дБм	CDMA	384 Kbps (deployed)– 2 Mbps	1–10 км
GPRS	900–1800 МГц	**Модуляція даних:** GMSK **Чутливість приймача:** -159 дБм	TDMA, FDMA, and FH	Up to 170 Kbps	1–10 км
Z-Wave/Z-Wave Alliance	900 МГц	**Модуляція даних:** FSK/BFSK (для 9,6 Кбіт/с і 40 Кбіт/с) GFSK (для 100 Кбіт/с) з BT = 0.6 **Чутливість приймача:** -104 дБм	CSMA-CA	9.6 Kbps–100 Kbps	100 м

Додаток Б

Міністерством освіти і науки України;
Тернопільський національний технічний університет імені Івана Пулюя (Україна);
Інститут електродинаміки НАН України (Україна);
Тернопільський обласний фонд ім. Івана Пулюя (Україна);
Інститут фізики напівпровідників ім. В.Є. Лашкарьова (Україна);
Харківський національний університет міського господарства імені О. М. Бекетова (Україна);
Warsaw University of Technology Lighting Technology Division (Польща);
Tallinn University of Technology (Естонія);
Universiti Brunei Darussalam Faculty of Integrated Technologies (Бруней);
Czech Technical University in Prague (Чехія);
Technical University of Košice (Словаччина)

VII Міжнародна науково-технічна конференція

„СВІТЛОТЕХНІКА й ЕЛЕКТРОЕНЕРГЕТИКА: ІСТОРІЯ, ПРОБЛЕМИ, ПЕРСПЕКТИВИ”

29-31 травня 2024 року
Тернопіль, Україна

УДК 004.7
Коваль М.О.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АРХІТЕКТУРА ТА ПРОТОКОЛИ ІНТЕРНЕТУ РЕЧЕЙ В РОЗУМНОМУ МІСТІ

M. Koval

IOT ARCHITECTURE AND PROTOCOLS IN A SMART CITY

Нові методології безперешкодно поєднують реальний і віртуальний світ, використовуючи деякі фізичні об'єкти та інтелектуальні давачі. Інтернет речей (IoT) - одна з таких методологій. Речі стають розумнішими, IoT дає користувачам можливість спілкуватися і контролювати фізичні пристрої, щоб надавати життєво важливу інформацію. Пристрої генерують та обмінюються великими обсягами даних, які, в свою чергу, допоможуть у прийнятті рішень.

Гаджети стали невід'ємною частиною нашого повсякденного життя, в тому числі вдома та на роботі. З появою передових технологій, таких як IoT, ми перебуваємо в режимі «підключеного» зв'язку з речами навколо нас. Такі досягнення дуже міцно увійшли в наше повсякденне життя. Завдяки IoT реальні речі стають частиною Інтернету, плавно поєднуючи фізичний та цифровий світ. Враховуючи все це, без жодних сумнівів можна сказати, що IoT - це "Майбутнє Інтернету". Переваги IoT незаперечні в кожній сфері життя. Розвиток Інтернету речей передбачає багато досягнень в «розумних містах», «розумних» будинках, цифровій охороні здоров'я та інших сферах [1]. IoT розширює можливості зв'язку та підвищує популярність мобільного зв'язку. IoT - це система, яка підтримує широкий спектр додатків з суперечливими вимогами та інтегрованими компонентами. Додатки IoT включають «розумну інфраструктуру», «розумну охорону здоров'я», «розумне управління», «розумну мобільність», «розумні технології» тощо. Попри всі ці переваги, послуги Інтернету речей повинні бути безпечними та надійними для повсякденного використання. Такі технології, як Bluetooth, ZigBee і технологія радіочастотної ідентифікації (RFID) забезпечують безпеку в IoT. Подолання технічних проблем вимагає ретельної оцінки рішень IoT.

З усіма технологічними досягненнями, IoT, безсумнівно, є кроком вперед у порівнянні з попередніми технологіями в кожній сфері життя, де задіяні технології.

Архітектура Інтернету речей враховує такі важливі фактори, як якість обслуговування (QoS), конфіденційність, надійність, цілісність тощо. У цьому розділі ми коротко розглянемо базову та сервіс-орієнтовану архітектуру IoT. Базова багаторівнева архітектура IoT запропонована в [2], [3] . Кожен архітектурний рівень коротко описується наступним чином: Рівень сприйняття складається з сенсорних пристроїв, а саме, RFID, ZigBee, коду швидкого реагування (QR) тощо, для загального управління пристроєм і збору конкретної інформації за допомогою кожного типу сенсорних пристроїв. Мережевий рівень пересилає інформацію з рівня сприйняття на верхні рівні і зберігає конфіденційність конфіденційної інформації від сенсорних пристроїв. Функції проміжного програмного забезпечення полягають в управлінні сервісами та зберіганні інформації нижнього рівня в базі даних. Прикладний рівень управляє додатками Інтернету речей, такими як "розумне здоров'я", "розумний транспорт" тощо. Бізнес-рівень охоплює управління всіма додатками та сервісами Інтернету речей

Література

1. Laghari, A. A., Wu, K., Laghari, R. A., Ali, M., & Khan, A. A. (2021). A review and state of art of Internet of Things (IoT). Archives of Computational Methods in Engineering, 1-19.
2. Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. Journal of Network and Computer Applications, 169, 102763.
3. Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C. P., Xiong, P., Iqbal, S., ... & Ghorbani, A. A. (2023). Internet of things (IoT) security dataset evolution: Challenges and future directions. Internet of Things, 100780.
4. Ghushe, H. Cross-layer design in the Internet of Things (IoT): issues and possible solutions.

УДК 621.391
Коваль М.О.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОГЛЯД ТА ВАЖЛИВІСТЬ СИСТЕМ НА ОСНОВІ LI-FI

M. Koval

OVERVIEW AND IMPORTANCE OF A LI-FI BASED SYSTEMS

Li-Fi розшифровується як Light-Fidelity (англ. «light» — «світло» і «fidelity» — «точність»). Оглянемо важливість системи на основі Li-Fi та порівнянню її продуктивності з існуючими технологіями. Li-Fi підходить для бездротової передачі даних з високою щільністю на обмеженій території та для вирішення проблем радіоперешкод. Li-Fi забезпечує кращу пропускну здатність, ефективність, доступність і безпеку, ніж Wi-Fi. Завдяки використанню світлодіодів та освітлювальних приладів існує багато можливостей для використання цього середовища: від публічного доступу до Інтернету через вуличні ліхтарі до автопілотованих автомобілів, які спілкуються через фари. У майбутньому ноутбуки, смартфони та планшети отримуватимуть доступ до даних через світло в кімнаті. Світло проникає майже скрізь, тому комунікація також може вільно йти разом зі світлом. Light Fidelity - це галузь оптичного бездротового зв'язку, яка є новою технологією. Li-Fi забезпечує бездротовий зв'язок всередині приміщень. Li-Fi - це передача даних за допомогою світла шляхом вилучення волокна з оптоволокна і надсилання даних за допомогою світлодіодного світла. Li-Fi - це нова технологія, яка використовує видиме світло для зв'язку замість радіохвиль. Основний принцип технології Li-Fi полягає в тому, що дані можуть передаватися за допомогою світлодіодного світла в дуже економічно ефективний спосіб. Інтенсивність світла змінюється навіть швидше, ніж людське око. У цю сучасну епоху її називають оптимізованою версією Wi-Fi. Він відноситься до систем зв'язку видимого світла 5G, що використовують світлодіоди в якості середньо- та високошвидкісного зв'язку, подібно до WI-FI [1]. Це допомагає економити велику кількість енергії, оскільки передача даних здійснюється через лампочки та інші освітлювальні прилади. У LI-FI світло використовується як носій, що є вдосконаленням електромагнітних радіохвиль, які використовуються у WI-FI. Однак воно не може проникати крізь стіни, на що здатні радіохвилі. Зазвичай це реалізується за допомогою білих світлодіодних ламп на передавачі низхідної лінії зв'язку [2]. Технологія Li-Fi працює подібно до оптоволоконної мережі, однак середовищем передачі є повітря/вільний простір. Сьогодні лазерне, інфрачервоне та ультрафіолетове випромінювання використовується для зв'язку по повітрю або у вільному просторі в різних системах. Для передачі даних в цій технології можуть використовуватися схеми модуляції OOK (On-Off Keying), OFDM. Для передачі даних за допомогою видимого світла необхідно увімкнути або вимкнути світлодіод. Коли світлодіод увімкнений, приймач розпізнає його як "1", а коли він вимкнений, приймач повинен розпізнати його як "0". Це не так просто, як надсилання та виявлення, для цього потрібно використовувати підсилювач/фільтр на стороні приймача. Найкраща частина комунікації видимого світла полягає в тому, що ми можемо скористатися перевагами високошвидкісної передачі даних і в той же час використовувати її для освітлення.[3], [4].

Література

1. HASANUDIN, Afif Hakim, et al. "From WI-FI to LI-FI: a comprehensive review of integration strategies." Przeglad Elektrotechniczny 2023.9 (2023).
2. Deval, Nimisha, et al. "Wireless Communication Using Light Fidelity Network." Techno-Societal 2020: Proceedings of the 3rd International Conference on Advanced Technologies for Societal Applications—Volume 1. Cham: Springer International Publishing, 2021.
3. Dahri, Faisal Ahmed, et al. "Design and implementation of LED–LED indoor visible light communication system." Physical communication 38 (2020): 100981.
4. Santosa, AA et. al. "An alternative dichromatic white LED light source for OOK-NRZ visible light communication system." Fourth International Seminar on Photonics, Optics, and Its Applications (ISPhOA 2020). Vol. 11789. SPIE, 2021.