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 протоколів взаємодії з IoT-пристроями при формуванні інформаційно-технологічних платформ

Виконав: студент VI курсу, групи САм-61
спеціальності 124 Системний аналіз
(шифр і назва спеціальності)

(підпис) Яєчник О.П. (прізвище та ініціали)

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

Нормоконтроль (підпис) Мацюк О.В. (прізвище та ініціали)

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

Рецензент (підпис) Гащин Н.Б. (прізвище та ініціали)

Тернопіль
2020

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)
«19» грудня 2020 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 124 Системний аналіз
(шифр і назва спеціальності)

студенту Яєчнику Олександру Петровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження протоколів взаємодії з IoT-пристроями при формуванні інформаційно-технологічних платформ

Керівник роботи Пасічник В.В., д.т.н., професор кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___» _____ 20___ року № _____

2. Термін подання студентом завершеної роботи 21 грудня 2020р.

3. Вихідні дані до роботи Наукові публікації та стандарти протоколів взаємодії з IoT-пристроями. Наукові публікації щодо організації інформаційно-технологічних платформ.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Інтернет речей – стан та перспективи досліджень. 1.1 Актуальність досліджень в галузі Інтернету речей. 1.2 Проблематика Інтернету речей. 1.3 Аналіз сучасного стану досліджень. 1.4 IoT-екосистема. 1.5 Висновки до першого розділу. 2 Стандарти та протоколи для Інтернету речей. 2.1 Протоколи передачі даних для IoT-пристроїв та систем. 2.2 IoT-протоколи маршрутизації мережевого рівня. 2.3 Протоколи інкапсуляції мережевого рівня IoT. 2.4 IoT-протоколи сеансового рівня. 2.5 Протоколи управління IoT-пристроями та системами. 2.6 Висновок до другого розділу. 3. Інформаційно-технологічної платформа та безпека IoT-систем. 3.1 Структура інформаційно-технологічної платформи для інтеграції та управління IoT-пристроями. 3.2 Протоколи та стандарти для убезпечення IoT-систем. 3.3 Проєкти для підвищення рівня безпеки IoT-пристроїв. 3.4 Висновок до третього розділу. 4 Охорона праці та безпека в надзвичайних ситуаціях. 4.1 Електробезпека робочих місць користувачів комп'ютерів. 4.2 Організація цивільного захисту на об'єктах промисловості та виконання заходів щодо запобігання виникненню надзвичайних ситуацій техногенного походження. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Титульна сторінка. Тема, Мета, Об'єкт, Предмет дослідження. Завдання дослідження. Актуальність досліджень. Порівняльна характеристика. IoT-екосистема. Множина протоколів. Протоколи передачі даних. IoT-протоколи сеансового рівня. Порівняння IoT-стандартів сеансового рівня. Протоколи управління Структура інформаційно-технологічної платформи для інтеграції та управління IoT-пристроями. Висновки. Доповідь завершено.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Дмитроца Л.П., доцент		
Безпека в надзвичайних ситуаціях	Стадник І.П., професор		

7. Дата видачі завдання 21 вересня 2020 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	21.09.20-27.09.20	*Виконано*
2.	Підбір наукових джерел щодо протоколів взаємодії з	28.09.20-04.10.20	*Виконано*
	IoT-пристроями та формування інформаційно-		
	технологічних платформ		
3.	Переклад та опрацювання наукових джерел щодо	05.10.20-11.10.20	*Виконано*
	протоколів взаємодії з IoT-пристроями та формування		
	інформаційно-технологічних платформ		
4.	Виконання дослідження щодо формування інформацій-	12.10.20-18.10.20	*Виконано*
	но-технологічних платформ, протоколів та стандарти		
	для убезпечення IoT-систем		
5.	Оформлення розділу «Інтернет речей – стан та	19.10.20-25.10.20	*Виконано*
	перспективи досліджень»		
6.	Оформлення розділу «Стандарти та протоколи для	26.10.20-01.11.20	*Виконано*
	Інтернету речей»		
7.	Оформлення розділу «Інформаційно-технологічної	02.11.20-08.11.20	*Виконано*
	платформа та безпека IoT-систем»		
8.	Виконання завдання до підрозділу «Охорона праці»	09.11.20-15.11.20	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	16.11.20-22.11.20	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	23.11.20-29.11.20	*Виконано*
11.	Нормоконтроль	30.11.20-05.12.20	*Виконано*
12.	Перевірка на плагіат	07.12.20	*Виконано*
13.	Попередній захист кваліфікаційної роботи	14.12.20	*Виконано*
14.	Захист кваліфікаційної роботи	21.12.20	

Студент _____ Яєчник О.П.
(підпис) (прізвище та ініціали)

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

АНОТАЦІЯ

Дослідження протоколів та формування інформаційно-технологічної платформи для управління IoT-пристроями // кваліфікаційна робота освітнього рівня «Магістр» // Яєчник Олександр Петрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кафедра комп'ютерних наук, група САм-61 // Тернопіль, 2020 // С. – 79, рис.– 9, табл. – 2, кресл. – , додат. – 2, бібліогр. – 115.

Ключові слова: безпека, IoT, пристрій, платформа, протокол, сумісність, управління даними.

Кваліфікаційна робота присв'ячена дослідженню протоколів взаємодії IoT-пристроїв та систем і формуванню інформаційно-технологічної платформи для управління IoT-пристроями. В першому розділі кваліфікаційної роботи розглянуто актуальність досліджень в галузі Інтернету речей. Висвітлено проблематику Інтернету речей. Проаналізовано сучасний стан досліджень в галузі. Описано IoT-екосистему. В другому розділі кваліфікаційної роботи розглянуто протоколи передачі даних для IoT-пристроїв та систем. Досліджено IoT-протоколи маршрутизації мережевого рівня. Описано протоколи інкапсуляції мережевого рівня IoT. Проаналізовано IoT-протоколи сеансового рівня. Висвітлено протоколи управління IoT-пристроями та системами. В третьому розділі кваліфікаційної роботи розглянуто опис сформованої на основі аналізу наукових джерел структури інформаційно-технологічної платформи для інтеграції та управління IoT-пристроями, спроектованої у вигляді девятирівневої моделі. Окремо розглянуто електробезпеку робочих місць користувачів комп'ютерів та описано організацію цивільного захисту на об'єктах промисловості.

ANNOTATION

Study of IoT interaction protocols in information-technological platforms development // qualification work of «Master» degree // Yaiechnyk Oleksandr Petrovych // Ternopil' Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, group SAm-61 // Ternopil, 2020 // P. – 79, fig.– 9, tables – 2, chair. – , annexes – 2, references – 115.

Keywords: security, IoT, device, platform, protocol, compatibility, data management.

The qualification work is devoted to the study of protocols of interaction of IoT-devices and systems and the formation of an information technology platform for the management of IoT-devices. The first section of the qualification work considers the relevance of research in the field of the Internet of Things. The problems of the Internet of Things are covered. The current state of research in the field is analyzed. The IoT ecosystem is described. The second section of the qualification work discusses data transfer protocols for IoT devices and systems. IoT-protocols of network layer routing are investigated. IoT network layer encapsulation protocols are described. Session layer IoT protocols are analyzed. IoT devices and systems control protocols are covered. The third section of the qualification work considers the description of the structure of the information technology platform for integration and control of IoT-devices formed on the basis of the analysis of scientific sources, designed in the form of a nine-level model. The electrical safety of computer users' workplaces is considered separately and the organization of civil protection at industrial facilities is described.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ACK (англ. Acknowledge) – підтвердження успішності отримання TCP-сегменту.

CARP (англ. Common Address Redundancy Protocol) – протокол резервування загальних адрес.

CEP (англ. Complex Event Processing) – комплексне опрацювання подій.

DDS (англ. Data Distribution Service) – служба поширення даних.

DECT (англ. Digital Enhanced Cordless Telecommunication) – технологія цифрового бездротового зв'язку.

GPS (англ. Global Positioning System) – система глобального позиціонування.

GIS (англ. Geo Information Systems) – геоінформаційні системи.

IEEE (англ. Institute of Electrical and Electronics Engineers) – інститут інженерів з електротехніки та електроніки.

IETF (англ. Internet Engineering Task Force) – відкрите міжнародне співтовариство проектувальників, учених, мережевих операторів і провайдерів.

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

MAC (англ. Media Access Control) – управління доступом до середовища.

MQTT (англ. Message Queuing Telemetry Transport) – спрощений мережевий протокол.

M2M (англ. Machine-to-Machine) – машино-машинна взаємодія.

NFC (англ. Near Field Communication) – технологія бездротового високочастотного зв’язку малого радіуса дії.

OMG (англ. Object Management Group) – група управління об’єктами.

OASIS (англ. Organization for the Advancement of Structured Information Standards) – глобальний некомерційний консорціум, який займається

розробкою, конвергенцією і ухваленням відкритих стандартів в рамках міжнародного інформаційного співтовариства.

PHY (абревіатура від англ. Physical layer) – фізичний рівень.

REST (англ. Representational State Transfer) – репрезентативна передача стану

RFID (англ. Radio frequency identification) – радіочастотна ідентифікація.

RPL (англ. Routing Protocol for Low-Power and Lossy Networks) – протокол маршрутизації для мереж з низьким енергоспоживанням та втратами.

QoS (англ. Quality of service) – якість обслуговування.

SDN (англ. Software-Defined Networking) – програмно-конфігурована мережа.

SOA (англ. Service-oriented architecture) – сервісно-орієнтована архітектура.

TDMA (англ. Time Division Multiple Access) – метод часового поділу одного фізичного каналу зв'язку.

WSN (англ. Wireless Sensor Network) – мережа бездротових давачів.

XMPP (англ. Extensible Messaging and Presence Protocol) – відкритий мережевий протокол для обміну повідомленнями та інформацією про присутність.

ВДТ – відеодисплейний термінал.

ЕОМ – електронно-обчислювальна машина.

НС – надзвичайна ситуація.

ЦЗ – цивільний захист.

ЗМІСТ

ВСТУП

Актуальність теми. Інтернет речей (IoT) останнім часом викликає підвищений інтерес дослідників. Традиційно лише кілька типів пристроїв мали можливість підключатися до Інтернету, але завдяки останнім розробкам у галузі RFID, NFC, «розумних» давачів та протоколів зв'язку щороку підключаються мільярди різнотипових пристроїв. Смартфони завантажують дані про місцезнаходження та встановлені застосунки. «Розумні» мережі завантажують відомості про постачання та споживання ресурсів. Ці пристрої щомиті ґенерують великі за обсягом набори даних. В процесі функціонування та підключення до Інтернету IoT-пристрої використовують обширний перелік мережевих протоколів та засобів. Крім того виробники IoT-пристроїв регулярно розробляють та вдосконалюють протоколи та засоби для їх функціонування та взаємодії в умовах обмежених для пристроїв обчислювальних та енерго-ресурсів. Завдяки динамічному розвитку галузі Інтернету речей, на даний час немає усталених та загальноприйнятих протоколів та засобів мережевої взаємодії IoT-пристроїв та систем. Відсутні загальноприйняті архітектури інформаційно-технологічних платформ. Тому аналіз протоколів для формування архітектури інформаційно-технологічної платформи з використанням IoT-пристроїв та систем є актуальним напрямком досліджень.

Мета і задачі дослідження. Метою кваліфікаційної роботи є підвищення ступеня повноти подання інформації щодо процесів, що відслідковуються з використанням IoT-пристроїв та систем шляхом розроблення архітектури інформаційно-технологічної платформи для їх інтеграції.

Для досягнення поставленої мети і вирішення сформульованої задачі слід було виконати наступні завдання:

– Подати опис IoT-екосистеми.

– Проаналізувати стандарти та протоколи для Інтернету речей.

– Сформувати архітектуру інформаційно-технологічної платформи для інтеграції та управління IoT-пристроями.

– Проаналізувати безпекові протоколи та стандарти для IoT-систем.

Об’єкт дослідження: процеси взаємодії IoT-пристроїв та систем.

Предмет дослідження: протоколи та засоби для мережевої взаємодії IoT-пристроїв та систем.

Методи дослідження. Для розв’язання поставлених в кваліфікаційній роботі завдань використано: методи, сформовані на основі системного аналізу, методи мережевої взаємодії, методи побудови інформаційно-технологічних платформ.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що отримав подальший розвиток метод формування багаторівневої інформаційно-технологічної платформи для збирання відомостей з використанням IoT-пристроїв та систем.

Практичне значення одержаних результатів. Розроблено прототип структури програмно-алгоритмічних комплексів для збирання відомостей з використанням IoT-пристроїв та систем.

Апробація результатів кваліфікаційної роботи. Основні положення та результати проведених досліджень доповідались та обговорювались на VIII науково-технічній конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2020 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковані у двох працях науково-технічної конференції (Див. додаток А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 115 найменувань та 1 додатку. Загальний обсяг кваліфікаційної роботи складає 79 сторінок, з них 53 сторінки основного тексту, який містить 9 рисунків та 2 таблиці.

1 ІНТЕРНЕТ РЕЧЕЙ – СТАН ТА ПЕРСПЕКТИВИ ДОСЛІДЖЕНЬ

1.1 Актуальність досліджень в галузі Інтернету речей

Інтернет речей (IoT) – одна з сучасних інформаційно-технологічних концепцій, яка пердбачає підключення кожного об’єкта (речі) у глобальну мережу, здатну здійснювати сенсорику, обмінюватися інформацією та виконувати аналітичне опрацювання для протреб різних типів застосунків [1]. Виникнення концепції IoT є результатом технологічної еволюції обчислювальних пристроїв та наслідком їх використання в різних сферах людської діяльності. Активне використання «розумних» об’єктів у повсякденному людському житті призвело до проектування та розроблення інструментів та методів підключення до глобальної мережі Інтернет. Це відбувається для підвищенні ефективності використання пристроїв при генеруванні та опрацюванні важливих та значущих даних, які можна ефективно відбирати, транспортувати, зберігати та аналізувати з використанням хмарних інформаційно-технологічних платформ [2].

IoT-пристрої використовуються у різних сферах людської діяльності, зокрема містобудуіванні [3], військовій справі, медицині [4], освіті, наукових дослідженнях, промисловості та спортивній галузі [5]. Прикладом практичного використання Інтеренту речей є інноваційна концепція «розумного будинку», котрий пропонує своїм власникам обширний перелік різноманітних послуг, зокрема контроль доступу, моніторинг систем будинку, безпекові функції та централізовано управління багаточисленними побутовими пристроями [6], [7]. Ця концепція ефективно застосовує підключення побутової техніки до мережі Інтернет та використання стандартних протоколів зв'язку. При цьому використовуються «розумні» давачі та відеокамери [8]. Ще одним прикладом використання IoT-пристроїв є «розумне» сільське господарство, яке ефективного використовує «розумні» давачі та RFID для зміни форми традиційного прийняття рішень при

вирощуванні сільськогосподарських культур. Використання IoT-пристроїв дозволяє фермерам безперешкодно та швидко отримувати відомості щодо обширного переліку різноманітних параметрів поля, зокрема вологості, опадів, температури та швидкості вітру. Що дає можливість приймати своєчасні, точніші та ефективніші рішення щодо підвищення продуктивності та, як наслідок, підвищувати якісні характеристики врожаю. Ще однією ключовою галуззю використання Інтернету речей є управління ланцюжками постачання для якої він був вперше створений в 1991 році [9]. IoT надає системам ланцюгів постачання інформацію про реальний час та стан кожного процесу та транзакції [10]. Використання «розумних» давачів та RFID дає змогу ефективно відстежувати відвантаження продукції та й полегшує контроль та управління мобільними пристроями та засобами. Сучасні дослідження демонструють, що найближчим часом відбуватимуться регулярні інновації додатків та послуг сформованих на основі Інтернету речей [11].

Формування Інтернету речей як інформаційно-технологічної галузі вимагає переосмислення традиційних принципів проведення обчислень. Для цього потрібні компактні, «розумні» та енергоефективні пристрої, які зможуть замінити традиційні обчислювальні машини. RFID, бездротові сенсорні мережі, «розумні» давачі, мобільні телефони, ноутбуки та портативні пристрої – основні інформаційні технології, які використосуються в якості складових елементів Інтернету речей [12]. RFID використовує мікросхеми, прикріплені до будь-якого відслідковуваного об'єкта для автоматичної ідентифікації, відстеження та бездротової передачі відомостей.

Мережа бездротових давачів та сенсорів (WSN) використовує невеликі обчислювальні вузли для пормування вимірювальних мереж та передачі інформації до кінцевого користувача [13]. Для моніторингу та отримання даних у режимі реального часу розгортаються тисячі вузлів. WSN пропонують апаратно-програмні рішення для широкого спектру застосувань у різних галузях, зокрема для медичного обладнання, моніторингу

характеристик навколишнього середовища промислового контролю виробничих потужностей та безпеки [14]. Фахівці прогнозують, що RFID та WSN будуть ключовими елементами інформаційних технологій на базі IoT.

Ще одним поширеним складовим елементом IoT є носимі обчислювальні пристрої, які використовуються для персональних обчислень. В короткочасовій переспективі носимі обчислювальні пристрої будуть використовуватися в сфері охорони здоров'я, бронювання та замовлення товарів та послут, освіті, спорті, індустрії розваг, управлінні видобуванням та постачанням ресурсів.

У медичній галузі IoT-пристрої використовуються для моніторингу артеріального тиску, частоти та характеристик серцебиття, прогнозування та дагностування захворювань за допомогою систем комп’ютерного зору та штучного інтелекту [15].

1.2 Проблематика Інтернету речей

На даний час описані вище інформаційні технології ефективно працюють для обмеженого набору програмно апаратних засобів, проте вони недостатньо інтегровані та, як наслідок недостатньо співпрацюють і розподіляють ресурси [16]. Серед невирішених задач в галузі Інтернету речей існує ряд проблемних областей, зокрема ідентифікація пристроїв, механізми взаємодії, проблеми стандартизації взаємодії між пристроями [17].

Концепція Інтернету речей дозволяє маленьким пристроям генерувати послідовні набори даних. Аналітичне опрацювання зібраних з використанням різнотипових пристроїв, протягом певного періоду часу, великих за обсягом наборів даних допоможе пиідвищити ефективність процесіва прийняття рішень [18]. IoT- пристрої будуть продукувати дані з дуже високою швидкістю і для зберігання зростаючих обсягів даних буде потрібна величезна кількість місця для зберігання. Окрім того проблемна область IoT-пристроїв значно ширша. IoT-пристроям притаманний найвищий рівень

неоднорідності природи пристроїв, виробників, стандартів зв'язку та розгортання застосунків. При цьому ґенеруються семантично різні дані різних типів та контексту. Інша провідна проблема в галузі Інтернету речей – це ефективне опрацювання та управління даними в різному контексті з метою вирішення обширного набору задач. По-третє, IoT-пристрої використовуватимуть безліч механізмів декодування, кодування та початкового опрацювання даних. По-четверте, архівування великих за обсягом наборів та колекцій даних з метою подальшого використання є актуальним завданням при розробленні застосунків на базі IoT-пристроїв.

Неоднорідна природа пристроїв IoT створює різні супутні завдання щодо процесів управління даними, формування рівнів їх абстракції, класифікації, стиснення, контролю доступу, архівування, взаємодії, забезпечення конфіденційність та захисту [19]. Тому на даний час актуальним завданням є формування комплексних систем збору та опрацювання даних з використанням IoT-пристроїв. Крім того, присутня потріба формування ефективних систем управління даними для семантичного аналізу та видобування зібраних за допомогою IoT-пристроїв даних. Важливо також зазначити, що сьогодні не існує зрілих рішень щодо управління даними для вирішення згаданих вище орієнтованих на IoT проблем. Хоча методи управління даними для окремих обчислювальних парадигм працюють добре. Але нам потрібно інтегрувати їх, щоб сформулювати рішення щодо вимог управління даними мережі Інтернет речей [20]. Решта статті впорядкована таким чином:

Інтернет речей (IoT) набуває популярності у промисловості та викликає інтерес в наукових колах. Концепція IoT передбачає що інтелектуальні пристрої можна розгорнути в будь-якому середовищі, де вони можуть взаємодіяти та кооперуватись з іншими пристроями. Це стало можливим завдяки недавньому розвитку Інтернет-протоколів, сенсорних пристроїв, ефективних обчислень, аналізу великих даних та засобів міжмашинної взаємодії (M2M). Згідно з доповіддю Гартнера, в найблищому майбутньому

IoT-технології очікують значні фінансові інвестиції та підвищений науковий інтерес [21].

1.3 Аналіз сучасного стану досліджень

Враховуючи дослідницький інтерес до інформаційних технологій сформованих з використанням IoT-пристроїв, щороку стандартизуються багато нових протоколів. Постійно публікуються нові наукові роботи, в яких висвітлюються різні аспекти стандартизації IoT-пристроїв та систем. Зокрема в статті [22] подано огляд стандартів IETF, а у [23] подано опис протоколів безпеки застосувань. В роботі [24] наведено огляд мережевих стандартів транспортного рівня. Автор статті [25] узагальнює найважливіші стандарти запропоновані організаціями до 2015 року. Він також подає обговорення IoT-проблематики, зокрема мобільності та масштабованості.

Основною причиною зростання величини обсягів даних, зґенерованих IoT-пристроями, є збільшення кількості пристроїв з підтримкою мережі Інтернет, які використовуються для різноманітних цілей приватними особами, бізнес-структурами та урядовими організаціями. Ці пристрої використовуються для аналізу даних, управління інформацією, створення та управління знаннями. Це допомагає ефективно реалізувати гнучну та своєчасну політику та приймати обгрунтовані управлінські рішення. Експоненційне зростання великий обсягів даних, породжених IoT-пристроями IoT, для ефективного опрацювання вимагає обґрунтованого та пропорційного збільшення обчислювальних потужностей. Крім того, дані, що генеруються пристроями IoT в різних доменах застосунків, є критичними щодо часу. Отже, своєчасне опрацювання даних Інтернету речей дуже вимоглива галузь досліджень та потребує врахування контексних можливостей пристрою та комплексного опрацювання подій (CEP). В таблиці 1.1 подано порівняльну характеристику сучасних інформаційно-технологічних платформ управління даними.

Таблиця 1.1 – Порівняльна характеристика сучасних інформаційно-технологічних платформ управління даними

Фреймворк/архітектура	Агрега-ція даних	Аналі-тичне опрацю-вання	Контек-сність	Гетеро-генніс-ть	Інтег-рація даних	Суміс-ність	Приват-ність	Видобу-вання знань
COIB-фреймворк [11]	Так	Так	Ні	Ні	Ні	Ні	Ні	Так
Сервіс-орієнтований фреймворк управління даними [26]	Так	Ні	Ні	Так	Ні	Так	Ні	Ні
Політична архітектура координації [27]	Ні	Ні	Так	Ні	Ні	Так	Ні	Ні
Центр даних, орієн-тований на дані [28]	Так	Ні	Так	Так	Ні	Ні	Ні	Ні
Широкомасштабне активне сховище на основі об’єктів [29]	Так	Так	Ні	Ні	Так	Ні	Ні	Ні
Інтелектуальна система управління сховищем [30]	Так	Так	Ні	Ні	Ні	Ні	Ні	Ні
Архітектура на основі Інтернету речей для підтримки мобільності [17]	Так	Ні	Ні	Ні	Так	Ні	Так	Ні

Група авторів на чолі з Кходададі у [28] пропонує інформаційно-технологічну платформу для розробки та розгортання програм IoT на основі хмарної інфраструктури. Запропонований фреймворк використовує сучасні модулі «Aneka» та приділяє додаткову увагу інноваційним функціям, необхідним для практичної реалізації IoT-застосунків. Для зв'язку між джерелами даних та платформою Aneka використовується протокол MQTT. Запропонована структура має три основні елементи: менеджер застосунків, хмарний менеджер та менеджер джерел даних. Менеджер застосунків розділений компоненти: компоновник застосунків, моніторинг, планувальник завдань та менеджер балансу навантаження. Ці компоненти надають користувачам базові функції для створення, планування та моніторингу програмно-алгоритмічних засобів. Хмарний менеджер використовується для опрацювання ключових аспектів, пов'язаних з хмарним сховищем даних IoT-пристроїв. Цей компонент виконує функції розподілу хмарних ресурсів,

масштабування ресурсів та моніторинг розподілених ресурсів підвищення загальної ефективності інформаційно-технологічної платформи. Менеджер джерел даних ключовим мостом між фреймворком та IoT-джерелами даних. Для опрацювання структурованих та неструктурованих даних в інформаційно-технологічній платформі використовується менеджер структурованих та неструктурованих джерел даних. Компоненти менеджера джерел даних можуть фільтрувати конкретні дані, надіслані з використанням IoT-джерел, відповідно до інформаційних запитів кінцевого користувача. Для зменшення мережевої затримки, менеджери джерел даних повинні використовуватися в безпосередній близькості від ресурсів даних. Автори розгорнули випробувальний стенд із п'ятьма віртуальними машинами на Amazon AWS для оцінювання продуктивності запропонованого фреймворку.

Інтернет речей – це інфраструктура, яка буде забезпечуватися численними різнорідними за своєю структурою та призначенням пристроями представленими у вигляді даних. Передані IoT-пристроями дані повинні мати сумісний із системою зберігання формат. Однак дані, створені IoT-пристроями, мають надмірність, аномалії та різний рівень абстракцій. Здебільшого, зґенеровані IoT-пристроями дані структуровані, напівструктуровані та неструктуровані. Для вирішення проблем структурування даних Базольд [31] пропонує когнітивно-орієнтовану структуру великих даних IoT (COIB-фреймворк).

Запропонована структура охоплює обширний перелік компонентів, зокрема фізичні пристрої, логічні IoT-сегменти, агрегатори та класифікатори великих даних зібраних з використанням IoT-пристроїв, HBase-зберігання, аналіз великих даних та когнітивні рішення. Спочатку вихідні дані передаються з фізичних IoT-пристроїв. Оскільки дані на цьому етапі є надлишковими, непослідовними та аномалізованими, то агрегатори великих даних зібраних з використанням IoT-пристроїв використовуються для здійснення операцій злиття даних. На цьому етапі відбувається усунення невідповідності та аномалій даних для отримання стандартизованої

семантики даних. Потім класифікатори великих даних отрманих від IoT-пристроїв ґенерують кластери даних на основі різних їх атрибутів. Потім конфіденційні та персональні дані помічаються як секретні та зберігаються за допомогою системи зберігання HBase. На наступному етапі дані можна аналізувати, використовуючи інструментальні засоби когнітивного та обчислювального інтелекту. В результаті всього процесу формулюються рекомендації для прийняття ефективних рішень та плани дій відповідно до різних наборів заявок. Автори запропонували використання центрів обробки даних для широкомасштабного впровадження розробленої моделі. Центри обробки даних призначені для виконання операцій агрегування, класифікації та зберігання зібраних з використанням IoT-пристроїв вихідних даних.

Для задоволення зростаючих потреб міського населення інформаційно-технологічна концепція IoT дуже швидко змінює парадигми людського життя. Для цього потрібно зробити міста достатньо «розумними» для забезпечення ефективного управління всіма операціями в галузі транспорту, енергетичного та ресурсного оменеджменту, охороні здоров’я та освіті. Це дозволить забезпечити легкий та своєчасний доступ до інформації в режимі реального часу та підвищити якість надання послуг громадянам. Ґін в [32] запропонував архітектуру шумового відображення для фіксованої (бездротової мережі давачів) та мобільної інфраструктури (смартфони, транспортні засоби з «розумними» пристроями і давачами та інші портативні пристрої) у «розумних» містах. Запропонована архітектура складається з трьох рівнів. Нижній рівень складається з давачів, інтегрованих в міську інфраструктуру, будинки, дорожню інфраструктуру. Середній рівень складається з вузлів ретрансляції, здатних збирати, буферизувати та передавати інформацію, отриману з нижніх рівнів до верхніх. Верхній рівень виконує роль шлюзу для надсилання інформації, отриманої від середнього рівня, до хмарної інфраструктури. Для практичної реалізації архітектури мережі авторами використано два режими функціонування: режим даних низької щільності та режим високої щільності. При цьому хмарні

обчислювальні платформи, такі як Microsoft Azure та Manjrasoft Aneka, використовуються для взаємодії та аналізу даних отриманих з допомогою IoT-пристроїв в режимі реального часу. Дані, зібрані з використанням стаціонарної або мобільної інфраструктури, зберігаються в хмарному сховищі разом із часовими мітками. У статті подано приклад картографування шуму для потреб міських служб.

Фонсіка [27] запропонував архітектуру розподіленої складної обробки подій (CEP) для вирішення проблем із затримкою, віддаленим оновленням політики, мобільністю та глобальним системний підходом, для обробки даних з різнотипових географічно-розподілених IoT-пристроїв. Щоб вирішити проблему затримки, дані слід обробляти якомога ближче до IoT-пристрою або безпосередньо в пристрої. Для цього автори визначили правила та координаційну політику, які визначають де і в який час повинен відбуватись аналіз даних. Запропонована архітектура називається GiTo. У цій архітектурі для прийняття своєчасних рішень атрибути пристрою (наприклад, місце розташування, час автономної роботи та місцезнаходження) добре продумані, а розподілений механізм CEP стежить за системною політикою та критичними подіями, що відслідковуються з використанням IoT-пристроїв.

Архітектура інформаційно-технологічної платформи GiTo має вісім основних компонентів. Цими архітектурними компонентами є контексний менеджер – відповідальний за реалізацію поточного контексту пристрою. CEP двигун та менеджер зв’язку – використовуються для керування обміном даними між пристроями. Хендовер-менеджер використовуэться для збереження стану мережевих з’єднань та активного зв’язку. Менеджер реэстру зберігає інформацію кластера для пристрою. Менеджер баз даних призначений для використання бази знань системи, а HAL – для вирішення проблем сумісності платформи сформованої на базі IoT-пристроїв.

Дослідження Романа [33] зосереджені на діяльності щодо об'єднання даних, формуванні логічних висновків, забезпеченні процесу виявлення

знань та управлінні великими даними сформованими з використанням IoT-пристроїв. Автори надають рекомендації щодо видобування знань в IoT-системах.

В роботі [34] представлено когнітивну IoT-структуру для розширення можливостей семантичного аналізу зібраних даних, управління знаннями, процесу виявлення та прийняття рішень.

З проведеного аналізу наукових джерел можна зробити висновок, що жодна поточна система управління даними зібраними з використанням IoT-пристроїв не відображає концептуального вирішення виявлених проблем.

1.4 IoT-екосистема

Подана на рисунку 1.1 екосистема IoT складається із семирівневої моделі: площадка, придбання, взаємозв'язок, інтеграція, аналітика, програми та послуги. На найнижчому рівні площадки, або домені програми, може бути «розумна» мережа, «розумний» будинок або «розумна» охорона здоров'я, тощо. Другий рівень складається з давачів та «розумних» пристроїв, які можна розглядати як ядро програмно-алгоритмічного комплексу. Тип і розподіл давачів залежить від контексту їх бажаного застосування.

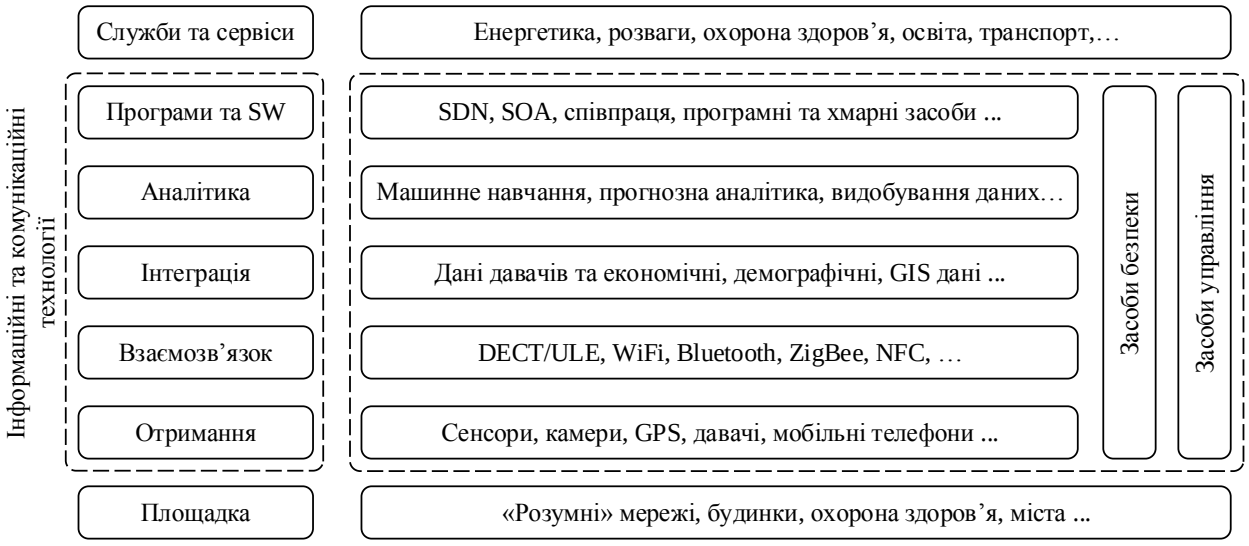

Рисунок 1.1 – IoT-екосистема [35]

Прикладами таких давачів є давачі температури, давачі вологості, «розумні» електричні лічильники або камери. Третій рівень складається з підрівня взаємозв'язку, який полегшує передачу даних від IoT-давачів до хмарного центру опрацювання даних. Там дані поєднуються з іншими відомими наборами даних, зокрема географічними, демографічними чи економічними даними. Крім того, об’єднані IoT-дані перевіряються за допомогою методів машинного навчання та аналітичного опрацювання даних. Для забезпечення масштабних розподілених обчислень присутня потреба розроблення нових програмно-алгоритмічних засобів для взаємодії та комунікації IoT-пристроїв. До таких парадигм належать програмно визначені мережі (SDN), архітектура, орієнтована на послуги (SOA), тощо. Верхній рівень може бути використано для формування результатів в галузі управління постачанням ресурсів та енергоносіїв, управління в галузі охорони здоров’я, транспорту, освіти, тощо. Кожен із запропонованих 7-шарів сформовано на основі нижніх рівнів.

Для формування та прототипування інформаційно-технологічної платформи опрацювання відомостей зібраних з використанням IoT-пристроїв потрібно дослідити протоколи, що використовуватимуться на різних рівнях взаємозв'язку IoT-екосистеми. Перелік та класифікацію протоколів подано рисунку 1.2 [35]. До них належать протоколи рівня передачі даних, мережевого та транспортного рівнів. Канал передачі даних з’єднує два елементи IoT, серед яких можуть бути два давачі або давач та шлюз, що з’єднує групу давачів з мережою Інтернет. Часто виникає потреба наявності декількох давачів для зв’язку та узагальнення інформації перед передачею даних в Інтернет. Спеціалізовані протоколи були розроблені для маршрутизації між давачами і є частиною мережевого рівня. Протоколи сеансового рівня дозволяють обмінюватися повідомленнями між різними елементами підсистеми IoT-зв’язку. Крім того, для IoT-пристроїв та систем розроблено декілька протоколів безпеки та управління.

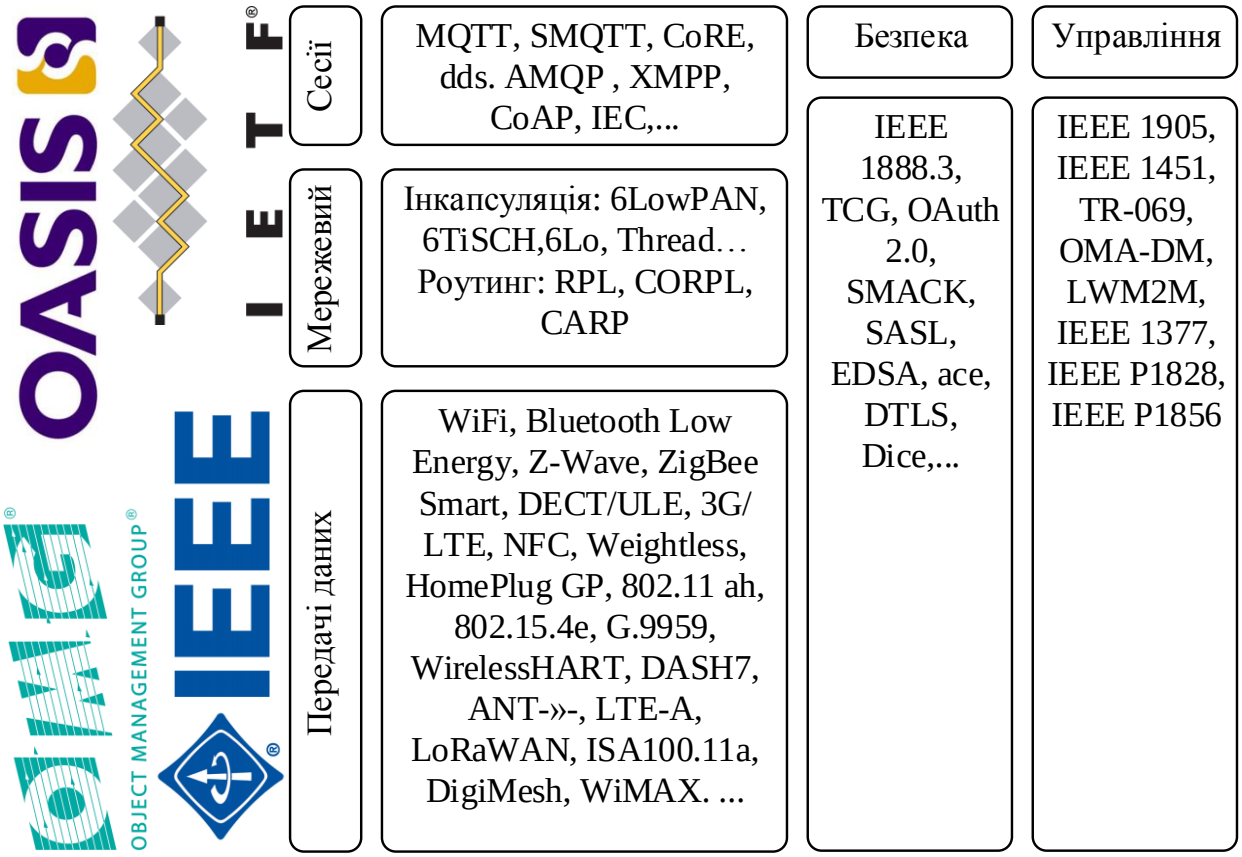

Рисунок 1.2 – Множина протоколів для IoT-пристроїв та систем

Стандарти, що охоплюють усі п’ять шарів поданих на рис. 1.1, запропоновано організаціями з стандартизації, зокрема IEEE, IETF та ITU. При цьому IEEE в основному працює над лінією передачі даних, IETF здебільшого стандартизує мережевий рівень, а декілька інших організацій працюють над стандартизацією сесій, безпеки та управління.

1.5 Висновки до першого розділу

В розділі розглянуто актуальність досліджень щодо Інтернету речей та описано проблематику галузі. Проаналізовано сучасний стан досліджень. Описано структуру IoT-екосистеми та наведено перелік використаних для її реалізації протоколів. На основі поданих в розділі відомостей можна зробити висновок, що оскільки постійно з’являються нові стандарти, то присутня потреба аналізу сучасного стану протоколів для IoT-пристроїв та систем.

2 СТАНДАРТИ ТА ПРОТОКОЛИ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

У цьому розділі подано опис стандартів і протоколів для передачі даних між IoT-пристроями та системами, що включає фізичні (PHY) та протоколи рівня MAC, які поєднуються за більшістю стандартів.

2.1 Протоколи передачі даних для IoT-пристроїв та систем

IEEE 802.15.4 – це стандарт передачі даних, який зазвичай використовується на рівні MAC. Стандарт визначає формат кадру, заголовки, адреси призначення та джерела та визначає, як може відбуватися зв'язок між вузлами. Традиційні формати кадрів, що використовуються в мережі, не підходять для пристроїв з обмеженим енергоспоживанням. Він використовує синхронізацію часу та перестрибування каналів для забезпечення високої надійності та низької вартості зв'язку ари передачі IoT-даних. Його MAC-особливості можна узагальнити наступним чином [36]:

– Структура слот-фрейму дозволяє планування та присвоєння стану вузлів у визначений час визначається структурою кадру IEEE 802.15.4e. Вузол може перебувати у стані сну, передачі або прийому. У сплячому режимі вузол вимикає радіо для економії енергії та зберігає всі повідомлення, які йому потрібно надіслати при наступній можливості передачі.

– Алгоритм планування може бути визначений розробником на основі потреб програмних засобів, однак планування має відповідати вимогам мобільності та передачі, які приймаються стандартами.

– Синхронізація вузлів необхідна для підтримки зв’язку вузлів із сусідами та шлюзом. Це можна зробити за допомогою синхронізації на основі підтвердження або на основі кадру.

– Перехід до каналу було запроваджено в IEEE802.15.4e, щоб дозволити часовий доступ до бездротового носія з використанням перестрибування каналів із часовим інтервалом (TSCH). Це вимагає зміни

частоти за допомогою заздалегідь визначеної випадкової послідовності, довільної довжини, може доходити до 511 елементів і охоплювати всі або підмножину каналів, доступних для фізичного рівня.

– Формування мережі та запити на приєднання – дві важливі вимоги до будь-якого протоколу MAC. У 802.15.4e вузли слухають широкосмугові команди і, отримавши принаймні одну таку команду, можуть надіслати запит на приєднання до широкосмугового пристрою.

IEEE 802.11ah – це найменша версія стандартів IEEE 802.11, яка є легкою для задоволення потреб IoT-пристроїв та систем. Стандарти IEEE 802.11 (також відомі як Wi-Fi) є найбільш часто використовуваними стандартами бездротового зв'язку в традиційних мережах. Вони широко прийняті для всіх цифрових пристроїв, включаючи ноутбуки, мобільні телефони, планшети та цифрові телевізори. Однак оригінальні стандарти WiFi не підходять для додатків IoT через витрати на кадрування та велике енергоспоживання. Тому робоча група IEEE 802.11 ініціювала групу завдань 802.11ah з метою розробки стандарту, який підтримує низькі енерговитрати, зручні для обміну даними між давачами та монітами [37]. Особливості MAC-рівня IEEE 802.11ah включають:

– Кадр синхронізації. Тільки діючі станції з актуальною інформацією про канал можуть передавати дані, резервуючи середовище канал. Станція знає, що може передавати, якщо правильно приймає пакет полів тривалості.

– Ефективний двонаправлений обмін пакетами. Дозвіл як на висхідну, так і на нижчу лінію зв'язку між точками доступу та давачами є особливістю IEEE 802.11ah. Ця функція зменшує енергоспоживання, оскільки давачі переходять у режим сну, після передачі даних.

– Короткий MAC-кадр. IEEE 802.11ah зменшує розмір кадру з 30 байт у традиційному IEEE 802.11 до 12 байт.

– Нульовий пакет даних. Традиційні стандарти 802.11 мали кадри підтвердження (ACK) 14 байт без даних. Така функція додасть багато енерговитрат, особливо для IoT-пристроїв. 802.11ah вирішує цю проблему,

вводячи міні сигнал, який називається преамбулою та використовується замість ACK, маючи при цьому набагато менший розмір.

– Збільшений час сну. Оскільки стандарт розроблений для пристроїв з обмеженою потужністю, він дозволяє тривалий час сну та ввімкнення лише для виконання процедуробміну даними.

WirelessHART – це стандарт MAC-рівня, який працює над IEEE 802.15.4 PHY і використовує множинний доступ з розподілом часу (TDMA) у своєму MAC-сегменті. Він використовує вдосконалені алгоритми шифрування для опрацювання повідомлень та перевірки цілісності. Він безпечніший та надійніший за інші протоли. Архітектура WirelessHART (див. рисунок 2.1) складається з мережевого менеджера, менеджера безпеки, шлюзу для підключення бездротової мережі до дротових мереж, бездротових фізичних пристроїв пристроїв, точок доступу, маршрутизаторів та адаптерів.

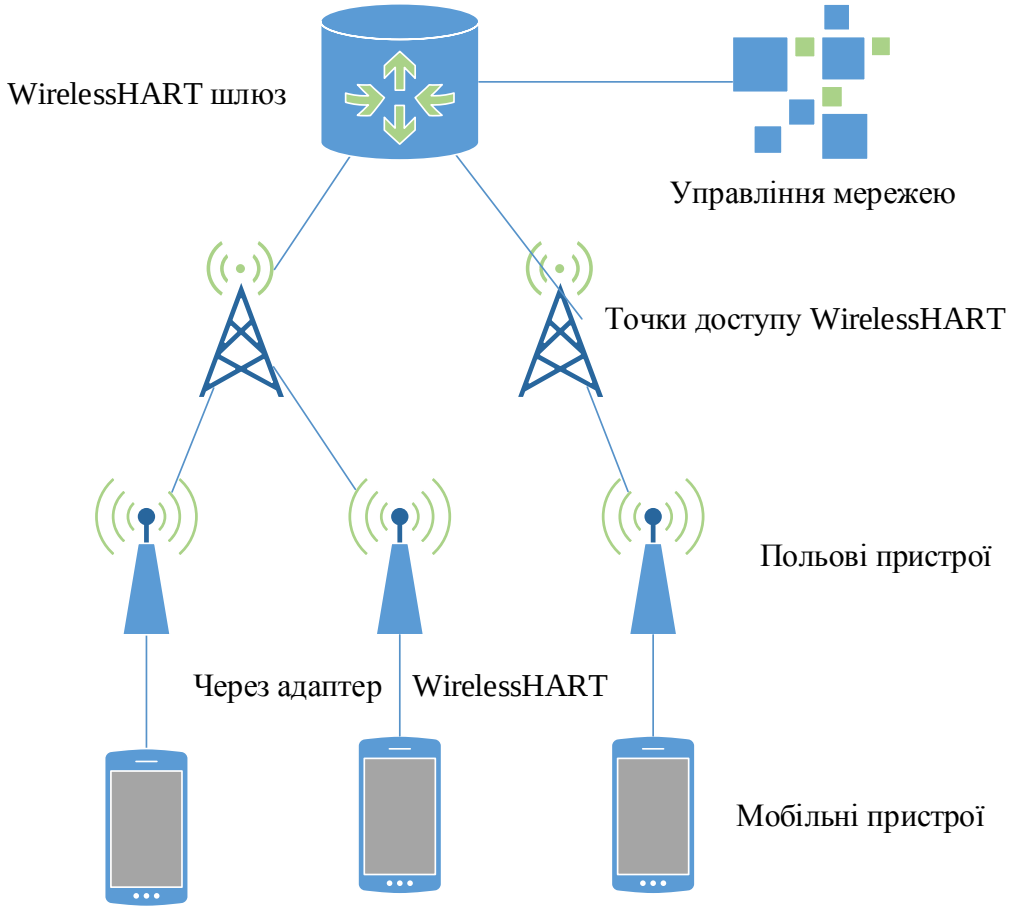

Рисунок 2.1 – Архітектура WirelessHART

Стандарт пропонує наскрізний, перехідний або одноранговий механізми безпеки [38].

Z-Wave – це стандарт MAC-рівня з низьким енергоспоживанням, який був розроблений для домашньої автоматизації, але нещодавно почав використовуватися в багатьох IoT-застосунках. Для зв’язку він охоплює відстань до 30-метрів від точки до точки і підходить для невеликих повідомлень. Стандарт використовує CSMA/CA для доступу до середовища передачі та процедури формування невеликих повідомлень ACK для забезпечення надійності передачі. Це слідує архітектурі ведучий/ведений, в якій ведучий управляє підлеглими, надсилаючи їм команди та обробляючи планування всієї мережі [39].

Іншим стандартом зв'язку короткого діапазону для рівня каналу передачі даних, який широко використовується в IoT-пристроях та системах, є Bluetooth з низьким енергоспоживанням або Bluetooth smart. Він в основному використовується в автомобільних мережах. Стандарт має невелику затримку, в 15 разів меншу за початковий Bluetooth. Енергоспоживання може бути в десять разів меншим, ніж у класичного Bluetooth. Контроль доступу використовує MAC без конфліктів з низькою затримкою та швидкою передачею [40].

ZigBee – це один із найбільш часто використовуваних стандартів в галузі Інтернету речей, який призначений для спілкування на середньому діапазоні в «розумних» будинках, пультах дистанційного керування та системах охорони здоров’я. Його мережеві топології включають зірку, однорангову ієрархію або дерево кластерів. Стандарт ZigBee визначає два профілі стека: ZigBee та ZigBee Pro. [41].

DASH7 – це новий протокол бездротового зв'язку, який використовується для активних пристроїв RFID і працює у загальнодоступній промисловій, науковій, медичній галузі. Він в основному розроблений для масштабованого покриття на відкритому повітрі на великій відстані з вищою швидкістю передачі даних у порівнянні з традиційним

ZigBee. Це недороге рішення, яке підтримує шифрування та адресацію IPv6. Його особливості MAC-рівня можна узагальнити наступним чином [42]:

– Фільтрування – вхідний кадр фільтрується за трьома процесами: перевірка циклічної перевірки надмірності (CRC), 4-бітна маска підмережі та оцінка якості посилання.

– Адресація – використовуються два типи адрес; унікальний ідентифікатор, який є ідентифікатором EUI-64, та динамічний ідентифікатор мережі, який є 16-розрядною адресою, вказаною адміністратором мережі.

– Формат кадру. MAC-кадр змінної довжини, що може становити максимум 255 байт, включаючи адресацію, підмережі, розрахункову потужність передачі та інші необов’язкові поля.

HomePlug GreenPHY (HomePlugGP) – це протокол MAC-рівня, розроблений HomePlug Powerline Alliance і в основному використовується в програмах домашньої автоматизації. Пакет HomePlug, включаючи HomePlug-AV, HomePlug-AV2, охоплює як PHY, так і MAC-рівні мережевого стеку. HomePlug-AV є основним протоколом зв'язку лінії електропередач, який використовує TDMA і CSMA/CA в якості протоколів MAC-рівня, підтримує адаптивне завантаження бітів, що дозволяє йому змінювати свою швидкість залежно від рівня шуму і використовує ортогональне мультиплексування з розподілом частоти (OFDM) і чотири методи модуляції.

HomePlugGP призначений для IoT-застосунків, зокрема «розумних» будинків та мереж. Він розроблений для зменшення вартості та енергоспоживання HomePlug-AV, зберігаючи при цьому його сумісність, надійність та покриття. Він використовує OFDM, як у HomePlug, але лише з однією модуляцією. Крім того, він використовує надійне OFDM-кодування для підтримки низької швидкості та високої надійності передачі. HomePlug-AV використовує лише CSMA як техніку рівня MAC, тоді як HomePlugGP використовує як CSMA, так і TDMA. Більше того, HomePlugGP має режим енергозбереження, що дозволяє вузлам спати, синхронізуючи час сну та прокидаючись при необхідності [43].

Довгостроковий розвиток (LTE-A) – це сукупність стандартів мобільних мереж, призначених для задоволення вимог M2M та IoT. Це один з найбільш масштабованих та економічно вигідних стандартів порівняно з іншими стільниковими протоколами. LTE-A був запущений у 2009 році з кількома випусками, які постійно надходять на підтримку нових технологій. Він традиційно використовує ортогональний множинний доступ з частотним поділом (OFDMA) як технологію середнього доступу, в якому частота поділяється на кілька піднесучих. Архітектура LTE-A складається з базової мережі (CN), мережі радіодоступу (RAN) та мобільних вузлів. CN відповідає за контроль мобільних пристроїв та відстеження їх IP-адрес. RAN відповідає за встановлення планів управління та передачі даних, а також за управління бездротовим підключенням та управлінням радіодоступом. RAN і CN спілкуються за допомогою лінії S1 (див. рисунок 2.2). RAN складається з eNB, до якого інші мобільні вузли підключені бездротовим способом [44].

Рисунок 2.2 – Архітектура LTE-A

Нові випуски LTE-A (LTE Rel-13 та Rel-14) представляють нові функції, розроблені з урахуванням перспективи вимог 5G [45]. Rel13 запропонував нові послуги для M2M-зв’язку, включаючи зниження енерговитрат, розширене покриття, позиціонування в приміщеннях та підтримку трансляції та багатоадресної передачі в одному сегменті. Очікується, що специфікація LTE Rel-14 ще більше вдосконалить FD-MIMO завдяки більшій кількості антенних порталів, надійнішій передачі та зменшенню зворотного зв'язку. Окрім того, очікується, що випуск стандартизує зменшення транспортний затримок та багатокористувацьку передачу по низхідній лінії зв'язку [46].

LoRaWAN – це нещодавно розроблена бездротова технологія широкосмугової мережі великого діапазону для IoT-застосунків. Це оптимізований протокол з низьким енергоспоживанням, розроблений для масштабованих бездротових мереж з мільйонами пристроїв. Він підтримує надлишкові операції, вільне розташування, низьку вартість, низькі енерговитрати та енергоощадні технології для підтримки перспективних IoT-потреб, забезпечуючи мобільність та зручність використання [47].

Weightless – ще одна нещодавно розроблена бездротова технологія для рівня IoT MAC, яку надає неприбуткова глобальна організація SIG. Можна використовувати два стандарти: невагомий-N та невагомий-W. Weightless-N був першим стандартом, розробленим для забезпечення IoT- вимог із використанням TDMA та зміною частоти для мінімізації перешкод. Він використовує надвузькі смуги в діапазоні ISM-частот до 1 ГГц. Weightless-W має такі ж функції, використовуючи телевізійний діапазон [48].

DECT – це універсальний європейський стандарт, призначений для бездротових телефонів. Нещодавно було надано розширення DECT/ULE (наднизька енергія), яке визначає низьке енергоспоживання та недорогий бездротовий інтерфейс, який можна використовувати IoT-застосунків. Він має спеціальне призначення каналів та має набагато більшу стійкість до перешкод та перевантажень [49].

EnOcean – це енергозберігаюча бездротова технологія, яка в основному використовується для автоматизації, але може бути використана для інших IoT-застосунків. Основна ідея полягає у використанні ефективного перетворення механічної або будь-якої іншої енергії та її перетворення в корисну. Цей протокол має відносно низький розмір пакетів і в основному використовується в IoT-застосунках для систем опалення, вентиляції та кондиціонування повітря [50].

На додаток до всіх раніше обговорених протоколів передачі даних, можуть використовуватися також зв’язок ближнього поля (NFC), ANT та стандарти Міжнародного товариства автоматизації (ISA100.11a). Ці стандарти мають обмежене використання для Інтернету речей. NFC використовується для зв'язку спеціально в короткохвильовому діапазоні. Він працює на відносно низьких частотах і використовує ідентифікатор радіочастоти для живлення приймача та запуску однорангової взаємодії [51]. ANT – це бездротовий протокол, який працює в режимі ведучого-веденого. Він в основному використовується для бездротових сенсорних мереж, працює на частотах 2,4 ГГц і концептуально схожий на низькоенергетичний Bluetooth [52]. ISA100.11a – це стандарти ISA, розроблені для бездротових мереж в галузі управління промисловою автоматизацією [53].

2.2 IoT-протоколи маршрутизації мережевого рівня

Протокол маршрутизації для IoT-мереж з низьким енергоспоживанням та з втратами (RPL) – це векторний протокол, розроблений в IETF для маршрутизації в IoT-системах. Він підтримує всі вище описані протоколи MAC-рівня та групу інших протоколів, які не призначені для IoT-пристроїв. Він базується на орієнтованих на орієнтовано-ациклічних графах (DODAG), які мають лише один шлях від кожного листового вузла до кореневого. Спочатку кожен вузол надсилає інформаційний об'єкт DODAG (DIO), що позиціонує себе в якості кореневого. DIO поширюється в мережі є матералом

для побудови DODAG. Під час спілкування об’єкт (DAO) надсилається від вузла батькам та поширюється до кореневого вузла. Кореневий вузол приймає вирішує, куди його скерувати, відповідно до пункту призначення. Нові вузли, які бажають приєднатись до мережі, надсилають запит інформації щодо DODAG (DIS). Після приєднання коренева система повертає підтвердження DAO (DAOACK). Вузли RPL можуть бути без приналежності, що є найпоширенішим їх станом. Вузол без приналежності відстежує лише батьківські вузли. Тільки root має повні знання про весь DODAG. Всі комунікації проходять через кореневий вузол root. Вузол зі станом відстежує свої дочірні та батьківські вузли. Взаємодіючи всередині піддерева DODAG, йому не потрібно проходити через кореневий вузол [54].

Когнітивний RPL, CORPL, – це протокол, який розширює RPL і використовує технологію DODAG, але з модифікаціями RPL. По-перше, він запроваджує опортуністичну переадресацію, яка дозволяє пакету встановити кілька пересилачів. Для переадресації пакету буде обрано лише найкращий наступний напрям. Потім кожен вузол буде підтримувати список переадресації замість батьківського та оновлювати список сусідів за допомогою повідомлень DIO. На основі оновленої інформації кожен вузол динамічно оновлює пріоритети сусідів будуючи набір адресатів [55].

CARP – це ще один протокол маршрутизації, який базується на розподілених мережах і призначений для підводного зв'язку. Це полегшений протокол переадресації пакетів. Його можна застосовувати до IoT-систем. Він враховує історичні вимірювання якості посилання для вибору маршруту переадресації. Ініціалізація мережі та пересилання даних – це два сценарії, які слід враховувати в таких протоколах. Під час ініціалізації мережі пакет HELLO транслюється з каналу на всі інші вузли в мережі. При переадресації даних пакет поступово передається від давача до потоку. Кожен наступний крок визначається самостійно.

Основна проблема CARP полягає в тому, що він не підтримує повторне використання раніше зібраних даних. Якщо програма вимагає даних давача

після суттєвих змін, то пересилання даних CARP не є вигідним. Покращення CARP було здійснено в E-CARP, дозволивши вузам зберігати раніше отримані сенсорні дані. Коли потрібні нові дані, E-CARP надсилає пакет пінгування, на який відповідають нові дані з вузлів давача. Таким чином, E-CARP різко зменшує накладні витрати на зв'язок [56].

2.3 Протоколи інкапсуляції мережевого рівня IoT

Звертання до IoT-пристроїв з довгими IPv6-адресами ускладнюється через обмеження довжини повідомлень при передачі IoT-даних. IETF розробляє набір стандартів форматування кадру для інкапсуляції датаграм IPv6 у малі фрейми каналів передачі даних, які використовуватимуться в IoT.

IPv6 через бездротову бездротову персональну мережу (6LoWPAN) є одним із перших і широко використовуваних стандартів IETF у цій категорії. Він ефективно інкапсулює довгі IPv6-заголовки у невеликі кадри MAC IEEE802.15.4 розмірами до 128 байт. Технічні характеристики 6LoWPAN надають багато можливостей, включаючи: адреси різної довжини, різні мережні топології, низьку пропускну здатність, низьке енергоспоживання, економічну ефективність, масштабованість мереж, мобільність, надійність та тривалий час сну. Стиснення заголовків використовується в стандартах для зменшення накладних витрат на передачу, фрагментації для досягнення 128-байтової максимальної довжини кадру в IEEE802.15.4 та підтримки багатоетапної доставки даних. Кадри 6LoWPAN використовують чотири типи заголовків: заголовок No 6loWPAN (00), заголовок диспетчеризації (01), заголовок сітки (10) та заголовок фрагментації (11). У випадку заголовка 6loWPAN будь-який кадр, який не відповідає специфікаціям 6loWPAN, відкидається.

6TiSCH – це ще один IETF-стандарт, розроблений робочою групою 6TiSCH. Він визначає способи передачі довгих IPv6-заголовків через режим TSCH-ліній передачі даних IEEE 802.15.4e. Цей режим зберігає доступні

частоти та їх часові інтервали в матриці, яка називається матрицею використання розподілу каналів. Матриця розділена на декілька фрагментів. Кожен фрагмент, будучи загальновідомим усім вузлам мережі, містить час і частоти. В межах однієї і тієї ж області перешкод вузли координують та узгоджують своє планування так, що всі можуть передавати без перерв. Планування стає проблемою оптимізації, коли часові інтервали присвоюються групі сусідніх вузлів, що використовують один застосунок. Стандарт не вказує, як можна зробити планування, і залишає це на розсуд конкретного застосунка для забезпечення максимальної гнучкості IoT-систем. Планування може бути централізованим або розподіленим залежно від програмних засобів або топології на MAC-рівні [57].

Нещодавно стіорена IETF-група працює над пропозицією набору стандартів щодо передачі кадрів IPv6 засобами мереж з обмежених ресурсами вузлів (6Lo). Незважаючи на те, що 6LowPAN та 6TiSCH були розроблені для інкапсуляції, для охоплення всіх стандартів каналів передачі даних потрібно більше стандартів. Тому для IEFT сформував 6Lo. На даний час більшість специфікацій 6Lo ще не доопрацьовані і знаходяться на різних стадіях проектування. Наприклад, IPv6 через мережі IEEE 485 Master-Slave/Token Passing (MS/TP), IPV6 через DECT/ULE, IPV6 через NFC, IPv6 через IEEE 802.11ah та IPv6 через бездротові мережі для автоматизації процесів промислової автоматизації (WIA-PA). Розробля'ться проектна документація для регламентування передачі датаграм IPv6 через відповідні канали даних [58].

IPv6 на G.9959 – стандарт, визначений у IETF RFC 7428, котрий визначає формат кадру для передачі пакетів IPv6 з використанням ліній передачі даних G.9959. У G.9959 унікальний 32-розрядний ідентифікатор домашньої мережі призначається контролером та 8-розрядним ідентифікатором хоста, який виділяється кожному вузлу. Локальна IPv6-адреса повинна бути побудована за допомогою 8-бітового ідентифікатора хоста, щоб її можна було стиснути у кадрі G.9959. Щоб вмістити пакет IPv6 у

кадри G.9959, використовується стиснення заголовка, аналогічне до 6lowPAN. RFC 7428 має функцію захисту, використовуючи для шифрування спільний мережевий ключ. Однак цього недостатньо для критично важливих щодо вимог безпеки програм, які повинні мати наскрізне шифрування та автентифікацію. Ці функції передані протоколам вищого рівня.

RFC 7668 [59] визначає формат IPv6 через Bluetooth з низьким енергоспоживанням. Він використовує більшість методів стиснення 6LowPAN. Фрагментація здійснюється на підрівні протоколу управління та адаптації логічного каналу (L2CAP) у Bluetooth. Таким чином, функція фрагментації 6LowPAN тут не використовується. Крім того, Bluetooth з низьким енергоспоживанням в даний час не підтримує формування багатокаскадних мереж на рівні зв’язку. Натомість центральний вузол виступає в ролі маршрутизатора.

2.4 IoT-протоколи сеансового рівня

На транспортному рівні TCP та UDP є домінуючими протоколами для більшості програм, включаючи IoT-застосунки. Однак потрібно кілька функцій розповсюдження повідомлень залежно від вимог IoT-програм. Бажано, щоб ці функції реалізовувались сумісними стандартними способами.

Транспорт телеметричної черги повідомлень (MQTT) – це стандарт OASIS представлений IBM [60]. Він забезпечує зв'язок між програмами та користувачами і мережею та зв'язками. Архітектура публікації подана на рисунку 2.3, де система складається з трьох основних компонентів: видавців, передплатників та брокера. У IoT видавці – це давачі, які підключаються до брокера з метою надсилання даних та повернення в режим сну. Абоненти – це програми, які зацікавлені певним контекстом або сенсорними даними. Тому вони підключаються до брокерів для отримання інформації при отриманні нових даних. Брокери класифікують сенсорні дані згідно контексту та надсилають їх відповідним абонентам.

Рисунок 2.3 – Архітектура MQTT

Розширення MQTT, захищений MQTT (SMQTT), було запропоновано в [61], для забезпечення полегшеного шифрування на основі атрибутів. Таке шифрування використовує функцію багатоадресної передачі, в якій одне повідомлення зашифровується і доставляється до кількох інших вузлів, що досить часто зустрічається в додатках IoT. Як правило, алгоритм складається з чотирьох основних етапів: налаштування, шифрування, публікації та дешифрування. На етапі налаштування абоненти та видавці реєструються у брокера та отримують головний секретний ключ відповідно до вибору розробником алгоритму генерації ключів.

Розширений протокол черги повідомлень (AMQP) – ще один стандарт OASIS, який був розроблений для фінансової галузі, працює над TCP та використовує архітектуру публікації/передплати, подібну до MQTT. Основна відмінність зазначених стандартів у тому, що брокер ділиться на два основні компоненти: обмін та черги (див. рисунок 2.4). Компонент обміну відповідає за отримання повідомлень видавця та розподіл їх по чергах відповідно до наперед визначених ролей. Абоненти підключаються черг, які представляють теми, і отримують доступні сенсорні дані [62].

Рисунок 2.4 – Архітектура AMQP

Обмежений протокол застосунків (CoAP) є протоколом сеансового рівня, розроблений у робочій групі RESTful (Core) IETF, призначений для забезпечення інтерфейсу RESTful (HTTP) з низькими накладними витратами. REST – це стандартний інтерфейс, який широко використовується в сучасних веб-застосунках. Однак REST має значні накладні витрати та енергоспоживання, що зробило його непридатним для IoT-платформ. CoAP призначений для вирішення проблем REST та надання IoT-застосункам можливості використовувати служби RESTful, відповідно до їх вимог. Замість TCP протокол сформовано на UDP разом з полегшеним механізмом забезпечення надійності. Архітектура CoAP розділена на два основних підрівні: обмін повідомленнями та запит/відповідь. Підшар обміну повідомленнями відповідає за надійність та дублювання повідомлень, тоді як підшар запиту/відповіді відповідає за зв'язок.

Як показано на рисунку 2.5, CoAP може мати чотири типи обміну повідомленнями: підтверджуваний, непідтверджуваний, зворотний зв’язок та окремий.

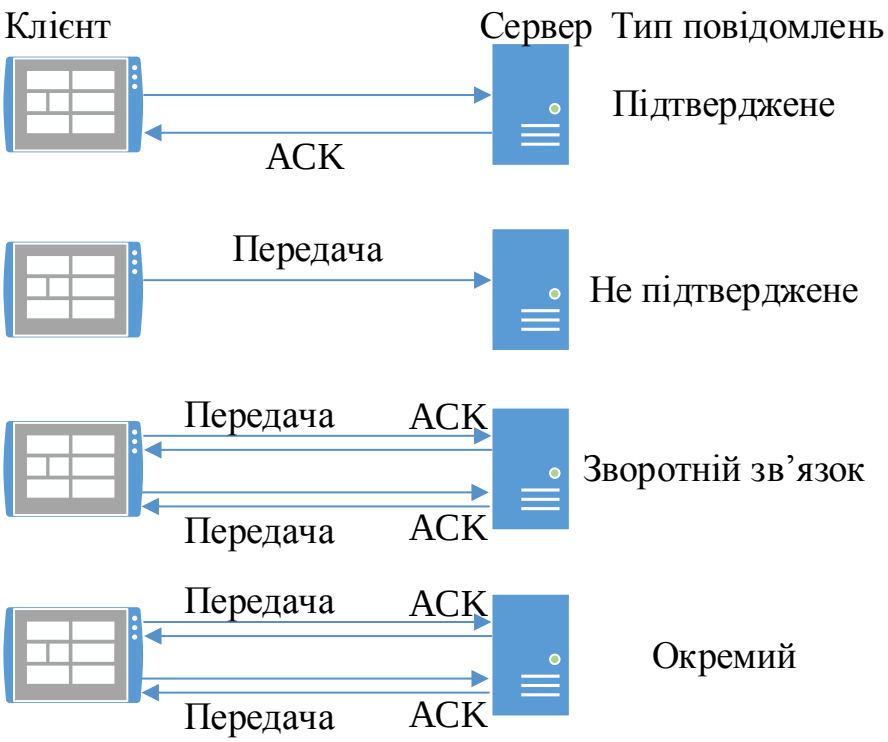

Рисунок 2.5 – Повідомлення CoAP

Підтверджуваний та непідтверджуваний представляють відповідно надійні та ненадійні передачі, тоді як інші режими використовуються для запиту/відповіді. Зворотній зв'язок використовується для прямої клієнт/серверної взаємодії, де сервер безпосередньо надсилає відповідь після отримання повідомлення, в межах повідомлення про підтвердження. Окремий режим використовується, коли відповідь сервера надходить із повідомленням, окремим від підтвердження, і може знадобитися деякий час для надсилання сервером. Як і в HTTP, CoAP використовує отримання, розміщення, надсилання, видалення запитів повідомлень для отримання, створення, оновлення та видалення даних [63].

XMPP – це протокол, який спочатку був розроблений для чатів та програм обміну повідомленнями. Він заснований на мові XML і був стандартизований IETF більше десяти років тому. Недавно його використання було розширено для IoT-застосунків та SDN завдяки стандартизованому використанню XML. XMPP підтримує архітектуру

публікації/підписки та запиту/відповіді. Розробник зстосунків повинен вибрати, яку архітектуру використовувати. Він розроблений для додатків у режимі майже реального часу та ефективно підтримує невеликі повідомлення з малим часом затримки. Протокол не забезпечує жодних гарантій якості обслуговування і, як наслідок, не є практичним для M2M-зв'язку. Повідомлення XML створюють додаткові накладні витрати завдяки великій кількості заголовків та форматів тегів, які збільшують критичне для IoT енергоспоживання. XMPP рідко використовується в Інтернеті речей [64].

DDS – це стандарти обміну повідомленнями, розроблені OMG. Вони використовують архітектуру публікації/передплати та в основному використовується для зв'язку M2M [65]. Накориснішими властивостями цього протоколу є надзвичайна якість рівня обслуговування та надійність із використанням без посередницької архітектури, яка підходить для IoT та M2M. DDS пропонує 23 рівні якості обслуговування, що дозволяють пропонувати різноманітні критерії якості, включаючи: безпеку, терміновість, пріоритет, довговічність, надійність, тощо. DDS визначає два підрівні: орієнтована на дані публікація-передплата та реконструкція локальних даних на підшари. Перший відповідає за доставку повідомлень передплатникам, а другий є необов'язковим і дозволяє просту інтеграцію DDS у прикладний рівень.

Подані вище стандарти повністю залежать від застосування. MQTT є найбільш широко використовуваним у IoT-застосунках через його низькі накладні витрати та енергоспоживання. Вибір стандартів залежить від організації IoT-застосунків. Наприклад, якщо програмні засоби побудовано з використанням XML то можна прийняти трохи накладних витрат у заголовках і XMPP може бути найкращим варіантом для вибору серед протоколів сеансового рівня. З іншого боку, якщо програмні засоби мають накладні витрати та чутливі до обчислювальних потужностей, тоді вибір MQTT буде найкращим варіантом. У таблиці 2.1 узагальнено порівняння між протоколами сеансового рівня.

Таблиця 2.1 – Порівняння IoT-стандартів сеансового рівня

Протокол	UDP/TCP	Архітектура	Безпека та QoS	Розмір заголовка (байт)	Макс. довжина (байт)
MQTT	TCP	Публ./Підп.	І те і те	2	5
AMQP	TCP	Публ./Підп.	І те і те	8	-
CoAP	UDP	Запит/Відп.	І те і те	4	20 (типово)
XMPP	TCP	І те і те	Безпека	-	-
DDS	TCP/UDP	Публ./Підп.	QoS	-	-

Якщо програмні засоби вимагають REST-функціональності та базуються на HTTP, тоді CoAP буде найкращим та чи не єдиним варіантом.

2.5 Протоколи управління IoT-пристроями та системами

Протоколи управління відіграють визначну роль в Інтернеті речей через різноманітність та вимоги до різних рівнів функціонування мереж. Потреба в неоднорідному та простому зв’язку між протоколами на одному або різних рівнях є критичною для IoT-застосунків. Існуючі стандарти в основному полегшують зв’язок між протоколами на одному рівні, і все ще залишається проблемою для зв’язку на різних рівнях функціонування IoT.

IoT має багато різних протоколів MAC-рівня. Отже, взаємодія між цими стандартами є критичною. Стандарт, розроблений IEEE, мав би забезпечити таку взаємодію, формуючи рівень абстракції поверх усіх різнорідних MAC-протоколів [66]. Ця абстракція дозволяє різним протоколам обмінюватися інформацією, приховуючи їх різноманітність та не вимагаючи жодних змін у їх конструкції. Рівень абстракції дозволяє обмінюватися повідомленнями, які називаються блоками даних керуючих повідомлень (CMDU), серед усіх стандартних пристроїв. Як показано на

рисунку 2.6, усі пристрої, сумісні з IEEE 1905.1, розуміють загальний протокол "управління абстракцією (ALME)", який пропонує обширний перелік послуг, включаючи: виявлення сусідів, обмін топологіями, повідомлення про зміну топології, обмін статистикою трафіку, правила переадресації та асоціації безпеки.

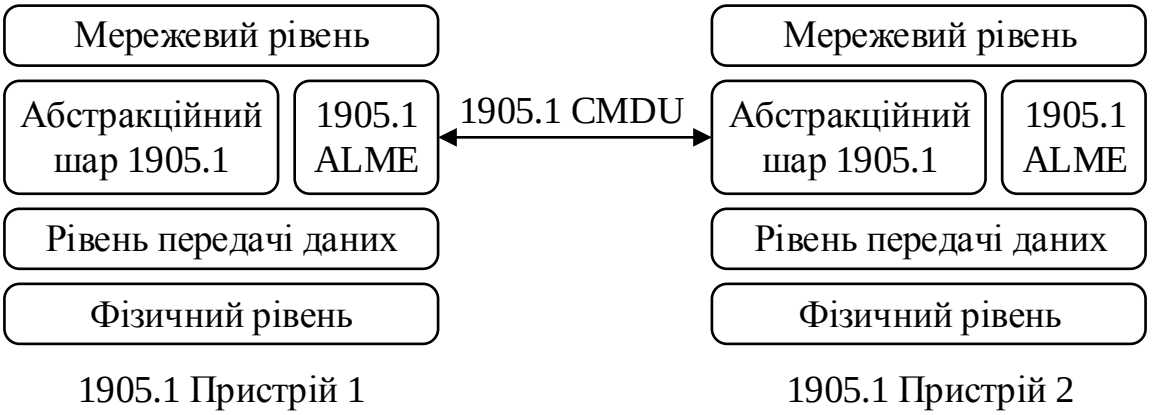

Рисунок 2.6 – Структура протоколу IEEE 1905.1

Інтелектуальний інтерфейс перетворювача – ще один стандарт, який надано IEEE 1451 і використовується для полегшення управління різними аналоговими перетворювачами та давачами. Ідея цього інтерфейсу полягає у використанні ідентифікації plug and play за допомогою стандартизованих електронних таблиць перетворювачів (TEDS). Кожен перетворювач містить TEDS, який включає всю інформацію, необхідну системі вимірювань, включаючи ідентифікатор, характеристики та інтерфейс пристрою. Аркуші даних зберігаються у вбудованій пам'яті сенсора або давача та мають визначений механізм кодування для розуміння великої кількості типів давачів та програм. Використання пам’яті мінімізується за допомогою використання невеликих XML-повідомлень, які доступні різним виробниками та програмам [67].

Технічний звіт 069 “CPE (обладнання для клієнтів), протокол управління глобальною мережею (CWMP)”, це розроблена Широкосмуговим форумом галузева специфікація, призначена для віддаленого управління

M2M-пристроями за допомогою HTTP-повідомлень. У цій специфікації управління здійснюється за допомогою http-повідомлень, що надсилаються клієнтам або пристроям із сервера. Специфікація є критично важливою для M2M-пристроїв, але оскільки вона базуэться на http-повідомленнях то на даний час має обмежене використання для IoT-застосунків [68].

Управління пристроями OMA – це протокол, розроблений Open Mobile Alliance (OMA). Він використовується для віддаленого забезпечення, оновлення та управління проблемами несправних M2M-пристроїв. Протокол використовує XML-повідомлення для зв'язку через http. Його можна використовувати для будь-якого транспортного протоколу на основі XML, наприклад XMPP. Однак повідомлення в такому протоколі все ще є складними для використання обмеженими ресурсами IoT-пристроїв [69].

Легкий M2M – ще один протокол OMA, спеціально розроблений для управління IoT-пристроями. Цей клієнт-серверний протокол використовує JSON (JavaScript Object Notation) для обміну повідомленнями. Він здебільшого побудований на CoAP, але може застосовуватися до інших протоколів сеансового рівня. Цей протокол використовується для управління функціями IoT-пристроїв через мережу передачі даних із сервера на пристрої і може бути розширений до багатьох повідомлень сервер-клієнт [70].

2.6 Висновок до другого розділу

У цьому розділі описано та проаналізовано різні протоколи передачі даних для Інтернету речей. Ці протоколи в основному стандартизовані IEEE, ITU або іншими організаціями, що займаються стандартами бездротового зв’язку. Загалом, найпоширенішими стандартами для IoT є Bluetooth та ZigBee. З іншого боку, IEEE 802.11ah є найбільш сумісним із IEEE 802.11, який є найбільш часто використовуваною інфраструктурою в інших бездротових застосунках.

Розглянуто протоколи маршрутизації, які можна використовувати для IoT. Зокрема RPL – це стандартизований протокол векторів відстані і, найбільш часто використовуваний. CORPL – це нестандартне розширення RPL, яке призначене для когнітивних мереж і використовує опортуністичну переадресацію для пересилання пакетів. E-CARP є єдиним протоколом маршрутизації на основі вимірювання якості розподіленого каналу, який розроблений для мережевих застосунків на базі IoT-давачів.

Окремо розглянуто інкапсулювання довгих IPv6-датаграм у невеликі MAC-кадри для IoT-пристроїв. Спочатку описано 6LowPAN та 6TiSCH для IPv6 над 802.15.4 та 802.15.4e. Ці протоколи важливі, оскільки 802.15.4e є найбільш широко використовуваною структурою інкапсуляції, розробленою для IoT-пристроїв та систем. На наступному етапі подано коротку специфікацію 6Lo, що використовується для передачі IPv6-датаграм через різні механізми доступу до каналів із використанням стандартів 6LoWPAN.

Також подано опис протоколів управління. Розглянуто проблеми сумісності та неоднорідності різних IoT-протоколів. Зокрема IEEE-1905.1 використовується для опрацювання неоднорідності протоколів MAC-рівня, тоді як IEEE 1451 використовується для перетворювачів та управління IoT-давачами. TR-069, OMA-DM та LWM2M використовуються для протоколів віддаленого управління. Де LWM2M є більш придатним і широко використовується для IoT-систем. Управління між протоколами та убезпечення на різних рівнях зв’язку в IoT-системах – це проблема, яка потребує вирішення.

3 ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНОЇ ПЛАТФОРМА ТА БЕЗПЕКА IOT-СИСТЕМ

3.1 Структура інформаційно-технологічної платформи для інтеграції та управління IoT-пристроями

Діяльність з управління даними, зібраними з використанням IoT-пристроїв поділяється на декілька етапів. Розбиття діяльності з управління даними, зібраними з використанням IoT-пристроїв та систем на рівні призводить до спрощення, повноти та масштабованості функціональності систем сформованих за таким принципом [71]. Запропонована структура сприяє розширенню контекстних характеристик щодо відбору, управління та аналізу вимог Інтернету речей. Запропонована структура інформаційно-технологічних платформ та систем з використанням IoT-пристроїв, сформована на основі поданої в [72] та складається з дев'яти шарів (див. рисунок 3.1). Структура включає рівні відбору даних, рівень туманних обчислень, рівень управління цілісністю, рівень безпеки, рівень агрегування даних, рівень аналітичного опрацювання даних, рівень зберігання даних, рівень застосунків та рівень архівування. Кожен рівень стеку запропонованої структури використовується у наступних рівнях процесу управління даними.

Рівень відбору даних є першим шаром у запропонованій структурі. Цей шар використовується для відбирання даних, що надходять з різних джерел, і направляє їх на верхні шари для обробки [73]. Рівень відбору даних насамперед має справу з численними неоднорідними IoT-пристроями, які використовуються для сенсорики та генерування даних у різних середовищах. Основними IoT-пристроями, що задіяні на цьому рівні, можуть бути давачі, «розумні» пристрої, RFID-пристрої, носимі пристрої, пристрої зчитування штрих-кодів та пристрої відео-спостереження. Зібрані дані можуть бути подані у різних формах та форматах.

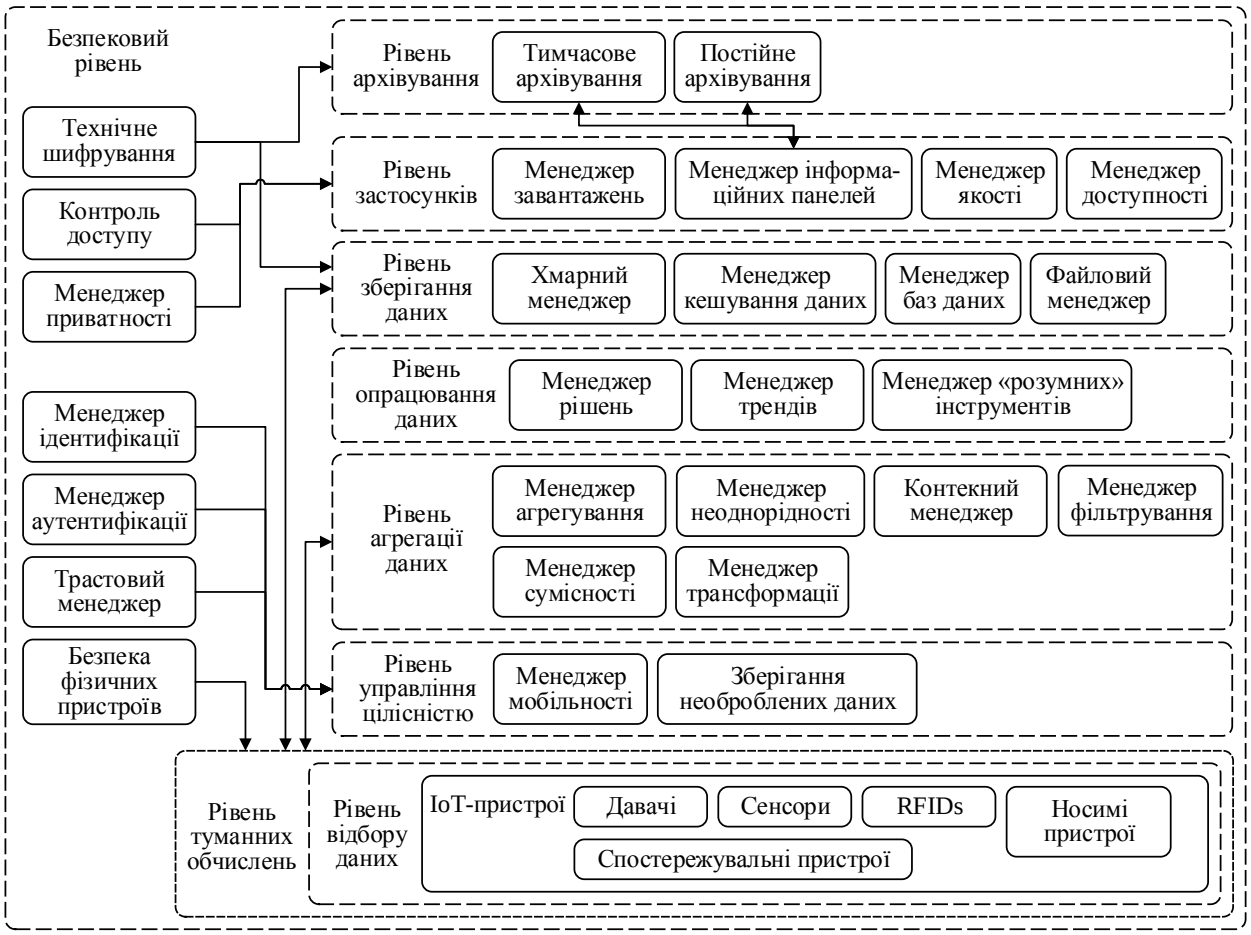

Рисунок 3.1 – Структура управління даними зібраними з використанням IoT-пристроїв та систем

Залежно від характеру програмно-алгоримічних реалізацій відбір даних може бути централізованим або розподіленим [74]. Зазначений шар подає дані для вищого шару туманних обчислень.

Рівень туманних обчислень є перспективним та критично важливим для часу виконання програмно-алгоритмічних комплексів. Він формує вимоги, згідно яких аналітичне опрацювання даних повинно виконуватись максимально наближено до місця їх генерації даних, та не відбувалось відправлявленя даних до хмарної інформаційно-технологічної платформи кожного разу для аналізу та прийняття рішень [75], [76]. Це вимагає перенесення функцій управління даними ближче до вимірювальних пристроїв. Тому в запропонованій структурній моделі передбачено рівень туманних обчислень, котрий забезпечує пристроям засоби для опрацювання,

аналізу та часткового зберігання даних на сусідніх вимірювальних вузлах. У запропонованій моделі рівень туманних обчислювальний в основному асоціюється з відбором, агрегацією та початковим зберіганням даних. Однак, з метою забезпечення функціональності управління даними на сусідніх низькорівневих вузлах, пристрої повинні мати вертикальну домінуючу ієрархію, обчислювальні потужності, пам’ять, час автономної роботи та всі інші необхідні ресурси. При цьому, лише критичні до часу дані агрегуються та аналізуються на пристроях, інакше вони надсилаються до хмарної платформи для довгострокового зберігання та аналітичного опрацювання.

Рівень управління цілісністю відповідає за комплексну цілісність процесу управління даними [77]. Основними компонентами цього рівня є зберігання необроблених даних та управління мобільністю. Для вирішення проблем, що викликають з мобільністю пристроїв у Інтернеті речей, менеджер мобільності відповідає за реалізацію функцій, пов’язаних із мобільністю пристроїв. Менеджер мобільності враховує вплив мобільності IoT-пристрою на контекст переданих даних. Менеджер мобільності використовує схеми підтримки мобільності послуг, сесій та особистої мобільності. Цей модуль відповідає за керування передачею даних між пристроями. Модуль зберігання необроблених даних управляє збереженням необроблених, великих за обсягом та неперервних потоків даних перед будь-якою операцією управління даними, виконаною на множині колекцій отриманих даних. Цей модуль використовує методи та інструменти для зберігання великих за обсягом потоків даних з підтримкою функціональних можливостей сховищ даних, метаданих та індексування збережених даних.

Щоб скористатися перевагами процесу управління даними, рівень управління цілісністю повинен реалізувати забезпечення автентичності, цілісності та доступності даних. Це зменшить накладні витрати на управління даними та не вплине на якість аналізу та рішень, прийнятих на основі цих зібраних даних.

Рівень агрегування даних призначений для зменшення їх розміру шляхом покращення процесів зберігання, організації та передачі даних [78]. Тому цей рівень призначений для узагальнення та об’єднання даних у режимі реального часу. Ключовими модулями рівня є менеджери фільтрування, неоднорідності, сумісності, агрегування, контексту та трансформації.

Дані, отримані від рівня управління цілісністю, є необробленими, надлишковими та дуже великими за обсягом. Їх потрібно попередньо опрацювати, перш ніж використовувати на рівні управління даними для аналітичного опрацювання. Фільтрування є основним етапом реконструкції даних та обробки подій. Фільтрування допомагає зробити необроблені дані відносно більш значущими та зменшити їх шумність. Менеджер фільтрації встановлює умови фільтрації для отриманих даних та виконує їх попереднє опрацювання. Засоби фільтрації можуть бути тимчасовими, постійними або сформованими на основі частоти необхідності. Їх також можна застосувати відповідно до вимог користувача та вимог застосунків.

Іншим компонентом рівня агрегування даних є менеджер неоднорідності. Неоднорідність пристроїв IoT створює проблеми управління через відсутність уніфікуючих підходів. У зв’язку з цим менеджер гетерогенності відповідає за опрацювання неоднорідності пристроїв, неоднорідності даних та семантичної неоднорідності. Для ефективності та простоти подальшого опрацювання потрібно виконати перетворення різнотипових даних, та різноманітних інтервалів вибірки в одиничні або множину попередньо визначених типів даних. Менеджер трансформацій відповідає за прозоре перетворення отриманих даних у формат перегляду користувацькими застосунками. На цьому етапі ключовими процесами є розділення, злиття та сортування даних.

Хоча запропонована структура IoT-систем з’єднує різнотипові та різнорідні пристрої, кваліфікована організація їх взаємодії важлива для забезпечення безперебійного зв’язку між пристроями та послугами. Тому повинні бути сформовані та визначені стандарти для представлення

пристроїв, пошуку та доступу. Для цього потрібно сформувати загальні стандарти взаємодії для обміну інформацією між IoT-пристроями різних постачальників. Менеджер сумісності повинен забезпечувати технічну, семантичну, синтаксичну та міждоменну сумісність.

IoT вимагає контексного збору та управління даними. Тому контекстний менеджер проводить пошук та вибір пристроїв, які могли б ґенерувати найбільш релевантні дані для користувацьких застосунків. Контекстний менеджер формує інформацію про контекст IoT-пристрою або групи IoT-пристроїв, що збирають дані в режимі реального часу. Підтримка специфікації контексту даних дозволить розробити нові послуги корисні для користувачів. Завдяки чому контексні дані легко та ефективно можуть бути доставлені користувачеві. Компонента працює для представлення контексту та моделювання. Менеджер контекстів повинен мати можливість ідентифікування нових контекстів, отриманих з попередніх даних.

Після забезпечення виконання вищевказаних процесів на рівні агрегування даних, менеджер агрегації опрацьовує та агрегує дані у формі, придатній для подальшої аналітики [79]. Для цієї мети використовується набір засобів агрегування даних для перевірки, обробки та агрегування даних у зазначеному форматі. Менеджер агрегації вибирає дані, які відповідають певним, наперед визначеним, принципам та стандартам.

Рівень безпеки використовується для забезпечення автоматизованої безпеки Інтернету речей. У запропонованій структурі рівень безпеки ґарантує забезпечення безпеки всіх рівнів і процесів управління даними та пов’язаний з усіма рівнями моделі. Він призначений для задоволення вимог безпеки на кожному окремому рівні. Відповідно до функціональних можливостей різних шарів моделі, цей рівень забезпечує відповідні інструменти захисту. Основними компонентами рівня безпеки є трастовий менеджер, менеджер аутентифікації, менеджер ідентифікації, засоби фізичної безпеки пристрою, методи шифрування, менеджер конфіденційності та контроль доступу.

Рівень цілісності підтримується такими модулями безпеки, як ідентифікація, автентифікація та менеджер довіри. Перевірка та ідентифікація джерел даних – одне з найважливіших завдань управління даними для IoT-пристроїв та систем. Кожному задіяному пристрою присвоюється ідентифікатор, а менеджер ідентифікаторів обробляє відповідні дані. Ця інформація пов’язана з процесом аутентифікації, що реалізується відповідним менеджером. Трастовий менеджер реалізує рівень довіри для всіх IoT-пристроїв. Рівень довіри пристроїв базується на їх правильності, повноті та своєчасності даних. Менеджер довіри періодично повторно обчислює та оновлює рівні довіри пристроїв, беручи до уваги поточну активність даних.

На рівні застосунків для виконання вимог безпеки використовуються менеджери контролю доступу та конфіденційності. Менеджер конфіденційності призначений для визначення політики конфіденційності застосунків [80]. Він забезпечує механізми захисту кінцевих користувачів від ризиків конфіденційності. Менеджер контролю доступу працює для контрольованого доступу до даних, пристроїв та облікових записів користувачів. В його обов'язки входить визначення прав власності на дані, безпечний обмін даними, розподілений доступ до даних та визначення дозволів на доступ до даних.

Для забезпечення захисту рівня зберігання даних та рівня архівування використовуються різні криптографічні методи та засоби шифрування. Механізми шифрування, що використовуються в шарі архівування, можуть бути обчислювально витратними та критично вимогливими до часу. Для забезпечення функціонування процедур отримання та зберігання даних під час їх виконання в IoT-програмах, методи шифрування на рівні зберігання даних не повинні бути обчислювально витратними та повинні забезпечувати безпеку даних.

Рівень аналітичного опрацювання даних збільшує значимість зібраних даних шляхом їх аналітичного опрацювання [26]. Цей рівень

використовується для задоволення потреб користувачів щодо ефективного інформування відповідно до оперативної ситуації з метою прийняття своєчасних та ефективних рішень про співпрацю з іншими користувачами та застосунками. Цей рівень повинен забезпечувати підтримку засобів аналітичного опрацювання даних для всіх типів та середовищ IoT, зокрема офлайн-засоби, динамічне середовище та середовище реального часу.

Рівень аналізу даних містить три модулі: менеджер рішень, менеджер тредів та менеджер «розумних» інструментів. Першим модулем рівня аналізу даних є менеджер рішень, який відповідає за керування рішеннями на основі поточних даних, отриманих з нижчих рівнів. Якщо користувачеві доводиться приймати рішення, пов’язані з проблемною областю, цей модуль враховуватиме поточні та історичні дані IoT-пристроїв, що стосуються цієї области, та ґенерує множину найбільш доречних рішень. Крім того, менеджер прийняття рішень періодично прийматиме стратегічні рішення на основі отриманих даних та передає їх відповідним організаціям та користувачам. Цей модуль допомагає користувачам у контексному прийнятті рішень щодо організації сутностей. Механізм прийняття рішень може бути корисним для застосунків фондової біржі, сільського господарства, прогнозування погоди та реального стану об’єктів. Менеджер трендів допомагає зрозуміти поточні тенденції та врахувати інтереси користувачів у різних сферах застосування. Менеджер трендів може знайти останні національні та міжнародні тенденції в галузях пов’язаних з молоддю, політикою, спортом та соціальними інтересами. Це сприяє пошуку тенденцій даних для кінцевих користувачів. Це дозволить організаціям краще зрозуміти вимоги користувачів відповідно до їх поточних інтересів та створити продукти відповідно до проведеного аналізу тенденцій. Це дозволить покращити ринкові прибутки та конкурентоспроможність.

Менеджер «розумних» інструментів використовується для управління засобами штучного інтелекту на рівні аналізу даних, котрі відіграють фундаментальну роль в прогнозних дослідження та при аналітичному

опрацюванні. Менеджер «розумних» інструментів використовує методи та засоби машинного навчання, нейронні мережі та інструменти видобування даних та знань для аналітичного опрацювання даних. Менеджер «розумних» інструментів забезпечиту сформованим на основі запропонованої моделі IoT-системам постійне формування нових аналітичних моделей та алгоритмів опрацювання наявних даних. Крім того, менеджер «розумних» інструментів працює над створенням автоматизованих інтелектуальних систем для виконання вимог аналітичного опрацювання та управління IoT-даними. Відповідно до потреб IoT-застосунків у режимі реального часу, необхідно постійно покращувати функціональність та швидкість роботи менеджера.

Рівень зберігання даних використовується для забезпечення потреб у стандартизованих та ефективних механізмах зберігання общирних та різноманітних наборів даних, що постійно генеруються у великих обсягах та кількостях. Рівень зберігання даних відповідає за їх збереження у режимі реального часу [29]. Цей рівень також вирішує проблеми з місцем зберігання даних, беручи до уваги характер даних та вимоги до програми. Іншим аспектом, який потребує розгляду на цьому рівні, є формат зберігання даних для різних типів даних, що надаються нижчими рівнями. Крім того, цей рівень також підтримує індексацію, каталоги та семантичні метадані збережених даних для своєчасного пошуку. Основними компонентами цього шару є хмара, кеш, база даних та менеджер файлів.

Хмарний менеджер застосовується для управління змарним сховищем, котре використовується організаціями як послугу та для організації власної інфраструктури сховища. Це забезпечить гнучкість та масштабованість зберігання даних. Для своєчасного та швидкого надання даних IoT-застосункам використовується менеджер кешування відповідальний за організацію та обслуговування кеш-пам’яті. Для різнорідних типів даних менеджер кеш-пам’яті відповідає за визначення політик кешування неоднорідних даних. Ці правила є загальними, за часом та за місцем

розташування. Менеджер кешування класифікує кешовані дані у формі категорій відповідно до вимог користувацьких застосунків.

Рівень застосунків призначений для надання послуг кінцевим користувачам та використовується для керування потоком даних. Прикладний рівень також виконує балансування навантаження. Цей рівень відповідає за підтримку якості обслуговування послуг та даних для кінцевого користувача [81]. Рівень аналізує та забезпечує доступність даних для доменів застосунків. Основними модулями цього рівня є менеджери завантажень, якості, інформаційних панелей, контролю доступу та доступності.

Менеджер балансування навантаження використовується для підтримки, керування, постійного забезпечення високого трафіку даних із різнорідних джерел та балансування навантаження. Менеджер балансування навантаження відіграє важливу роль у масштабованості, надійності та підвищенні продуктивності життєвого циклу управління даними отриманими з використанням IoT-пристроїв та систем. Цей модуль використовує політики маршрутизації та алгоритми розподілу запитів даних у джерелах, так що навантаження, що розподіляє між доступними ресурсами. Після фіксованого або довільного інтервалу цей компонент буде шукати надмірно та недостатньо використані ресурси для ефективного розподілу обчислювального навантаження. Балансування навантаження збільшує час роботи та доступність IoT-пристроїв з обмеженими енергоресурсами.

Для забезпечення послідовного та безперервного процесу ґенерації даних дуже важливо забезпечити наявність та доступність IoT-пристроїв. Доступність IoT-пристроїв робить можливим безперебійне, своєчасне та ефективне управління життєвим циклом даних. Менеджер доступності перевіряє наявність IoT-пристроїв і якщо деякі вимірювальні пристрої для певного застосунку не працюють, менеджер доступності досліджує інші пристрої, які можуть передавати дані замість недоступних джерел. Менеджер доступності намагається збільшити термін роботи IoT-пристроїв з

врахуванням наявних ресурсів. Ці два модулі прикладного рівня координуються так щоб менеджер доступності відстежував IoT-пристрої та їх ресурси на предмет використання обчислювальних потужностей, пам'яті та енергії. Ця інформація передається менеджеру балансування навантаження для розподілу навантаження та даних. Ця координація призводить до зменшення затримки обслуговування, мінімального часу простою та довгострокової доступності IoT-джерел даних.

Якість даних також має вирішальне значення для соціального та комерційного впливу на різні сфери застосування Інтернету речей. У зв’язку з цим IoT-дані повинні зберігати властивості повноти, коректності та якості інформації. Менеджер якості містить інструменти та техніки для визначення якісних характеристик даних для IoT-застосунків. Цей модуль проводить тестування IoT-пристроїв, платформ та відповідних інформаційних технологій. Менеджер інформаційних панелей допомагає користувачам керувати відповідними панелями застосунків, взаємодіяти, контролювати та візуалізувати бажаний вміст та послуги. Він полегшує користувачам налагодження власних інформаційних панелей в режимі реального часу. У запропонованій структурі інформаційна панель може координувати рівень агрегування даних за запитами користувачів.

Рівень архівування. Іншим важливим аспектом управління даними IoT-пристроїв та систем є архівування доступних великих обсягів генерованих та наявних даних. Рівень архівування відповідає за управління зростаючими потребами щодо архівування IoT-даних за допомогою масштабованої інфраструктури. Цей рівень підтримує індексування для ефективного та своєчасного пошуку даних. Цей рівень використовує алгоритмічні засоби для забезпечення незмінності та уникнення перепису. Шар архівування додатково розділений на два модулі – тимчасове та постійне архівування.

У запропонованій структурі інформаціно-технологічної платформи передбачено використання кешування найбільш часто доступних IoT-даних на рівні їх зберігання. Дані з відносно меншою частотою доступу тимчасово

архівуватимуться з використанням модуля архівування. Цей модуль використовується для управління та короткотермінового зберігання даних. Модуль призначено для керування політиками вибору низькопріоритетних та опрацювання застарілих даних з тимчасових архівів, для їх відправлення до модуля постійного архівування. Це передбачає прийняття рішень щодо формування вимог збереження різних типів доступних даних. Модуль постійного архівування призначений для зберігання даних впродовж необмеженого часу. Він використовує надлишкові криптографічні методи дотримання умов безпеки, довговічності та економічної ефективності. Крім того, зазначений модуль контролює доступ архівованого вмісту.

Після опису елементів запроносованої структури прототипу інформаційно-технологічної платформи для агрегації та опрацювання IoT-пристроїв та систем потрібно детальніше розглянути елементи їх безпеки.

3.2 Протоколи та стандарти для убезпечення IoT-систем

Для створення високого рівня безпеки інформаційно-технологічних платформ з використанням IoT-пристроїв та систем відповідна заходи слід розглянути на всіх описаних вище мережевих рівнях. Звичайні механізми безпеки, криптографія та інфраструктура відкритих ключів є недоцільними для IoT-платформ через їх складність та ресурсовитратність. На даний час розробляються нові стандарти щодо механізмів безпеки. Крім того, існують безпекові стандарти IoT.

Загрози безпеки IoT-пристроїв та систем охоплюють усі рівні, включаючи середовище передачі даних, мережевий, сеансови та застосунковий рівні. Протоколи 802.15.4e, WirelessHART, 6LoWPAN та RPL, пропонують певний безпековий функціонал для захисту взаємодії на відповідних рівнях.

MAC 802.15.4e пропонує різні режими захисту, використовуючи «безпекові біти» у полі управління кадру заголовків. Вимоги безпеки

стандарту включають конфіденційність, автентифікацію, цілісність, механізми контролю доступу та захищений синхронізований у часі зв’язок.

Стандарт WirelessHART забезпечує надійні функції безпеки, використовуючи найновіші та широко використовувані методи. Методи підтримують засоби унікальної безпеки кожного повідомлення на основі шифрування AES-128, цілісність даних та автентифікацію, зміну каналів захисту, індикацію невдалого доступу до IoT-даних та звіти про цілісність повідомлень та помилки автентифікації. Стандарт забезпечує різний рівень безпеки, залежно від програмно-алгоритмічних застосунків, використовуючи найновіші методи захисту.

В групі документів IETF щодо 6LoWPAN, обговорюються загрози, формуються вимоги до 6LoWPAN та запропоновано відповідні рішення. Зокрема у RFC 4944 обговорюються можливості дублювання адрес інтерфейсу EUI-64, які мають бути унікальними [82]. У RFC 6282 обговорюються питання безпеки, які порушуються через проблеми подані в RFC 4944 [83]. У документі RFC 6568 розглядаються механізми забезпечення безпеки в обмежених бездротових сенсорних IoT-системах та мережах [84]. В описі IoT-проектів [85], [86] подано механізми досягнення безпеки щодо 6loWPAN.

RPL пропонує різні рівні безпеки, використовуючи поле «Безпека» заголовків. Інформація в цьому полі вказує на рівень безпеки та криптографічний алгоритм, який використовується для шифрування повідомлення. RPL пропонує підтримку автентичності даних, семантичної безпеки, захисту від атак повтору, конфіденційності та управління ключами реалізуючи при цьому незахищений, попередньо встановлений та автентифікований рівні безпеки. Загрози RPL включають вибіркову переадресацію, буріння, Sybil, переповнення, червоточини та атаки з метою відмови в обслуговуванні. В документі RFC 7416 [87] подано обговорення загроз безпеці та можливі атаки на RPL, включаючи атаки на конфіденційність, доступність та цілісність з можливими заходами протидії.

Захист транспортного рівня (TLS) та датаграма TLS (DTLS) – два широко використовувані стандарти безпеки в галузі Інтернету речей. Вони в основному забезпечують автентифікацію, цілісність та конфіденційність на транспортному рівні, особливо що використовується в протоколах CoAP. TLS надає інструменти безпеки засобами TCP-передачі. DTLS надає інструменти засобами UDP та датаграм. TLS та DTLS складаються з двох підрівнів протоколів – запису та погодження – які відповідно реалізують інкапсуляцію та аутентифікацію. У RFC 7925 подано детальні механізми у цих стандартах для безпеки та забезпечення конфіденційності [88]. Зазначені стандарти можуть надавати облікові дані, підписи та засоби опрацювання помилок з використанням традиційних механізмів безпеки, модифіковані з урахуванням обмежених ресурсів IoT-пристроїв.

Стандарт IEEE 1888.3 [89] визначають вимоги до безпеки та механізми для повсюдного протоколу мережі управління зеленими спільнотами. Вимоги безпеки включають захист інформації, цілісність, конфіденційність, автентифікацію та контроль доступу. Стандарт надає рекомендації щодо архітектури та компоненти, необхідні для забезпечення безпеки IoT, визначаючи послідовність зв’язку та механізми безпеки, зокрема погодження, аутентифікацію та механізми контролю доступу.

TCG надає рекомендації щодо реалізації безпечних IoT-застосунків із використанням різних варіантів використання та механізмів безпеки, включаючи аутентифікацію за допомогою унікальних ідентифікаторів, захист від зараження проміжним програмним забезпеченням за допомогою TLS, а також доведену доступність, конфіденційність та цілісність із використанням різних методів. Зокрема методів реалізації довіри до оновлення (RTU) та модуль надійної платформи (TPM), які використовуються в сумісних з TCG пристроях [90]. Зазначені технічні характеристики призначені для допомоги IoT-розробникам у виборі механізмів захисту програм. Однак розробники повинні приймати рішення щодо збалансованості безпеки системи, складності та витрат ресурсів.

Система авторизації OAuth, подана в IETF RFC 6749 [91], дозволяє надійним стороннім серверам контролювати права доступу та дозволи ресурсів. Специфікація дозволяє клієнтам використовувати авторизацію та доступ у власників через сервер авторизації. Сервер перевіряє облікові дані клієнтів та права доступу та приймає рішення щодо доступу до ресурсів. Повідомлення базуються на HTTP, який рідко використовується для IoT-пристроїв та систем через його накладні витрати порівняно з іншими протоколами. RFC 6819 [92] описує додаткові заходи безпеки, які поширюють OAuth на нові моделі загроз. Автори [93] обговорюють загрози та відкриті питання безпеки, які виходять за рамки OAuth 2.0 і потребують вирішення в наступних версіях протоколу. Ці загрози включають витік облікових даних, ін’єкції та ризики на сторонніх серверах авторизації.

Простий рівень автентифікації та безпеки (SASL) – це ще одна система безпеки від IETF для підтримки аутентифікації в IoT-застосунках з використанням серверів. Він відокремлює програмні засоби від процесів аутентифікації та використовує прості повідомлення для аутентифікації клієнтів. Як правило для IoT-пристроїв ці засоби забезпечуються протоколами сеансового рівня, які підтримують TLS та SSL, зокрема, MQTT та AMQP [94]. Аутентифікація та авторизація в обмежених середовищах (ACE) – це механізм безпеки, призначений для IoT-пристроїв з обмеженими ресурсами. На відміну від OAuth він побудований на повідомленнях на основі CoAP. Слід зазначити, що специфікації нещодавно були затверджені в IETF RFC 7744 [95], [96].

Новим напрямком досліджень в галузі безпеки Інтернету речей є використання блокчейн при формуванні та інтелектуальних взіємодії IoT-платформ. Blockchain – це технологія розподіленої книги, яка дозволяє сформувати заходи безпеки проекту, не звертаючись до централізованого або довіреного органу у формі третьої сторони [97]. Технологія традиційно використовується для біткоїнів та інших віртуальних криптовалютних платформ. Недавно розпочато ряд досліджень у багатьох інших доменах,

включаючи Інтернет речей. IBM та інші виробники IoT-пристроїв розглядають можливість застосування інформаційно-технологічних Blockchain-рішень для формування їх безпеки [98]. Блокчейн можна використати для забезпечення умов конфіденційності IoT-платформ [99]. У роботі [100] автори обговорювали механізми безпечного обміну даними між IoT-пристроями та організаціями з використанням блокчейн. Формування інтелектуальних взаємодій з використанням блокчейн-технології обговорено в [101], а в [102] надано описи інформаційно-технологічних архітектур, сформованих на основі блокчейн-застосувань для IoT-платформ.

3.3 Проєкти для підвищення рівня безпеки IoT-пристроїв

Незважаючи на велику кількість запропонованих для Інтернету речей безпекових протоколів та стандартів, присутній високий рівень загрози зловмисних дій та залишається ряд невирішених проблем, що вимагають подальших досліджень.

Деякі з питань щодо IoT-безпеки обговорюються у декількох IETF-проектах. Зокрема, різні аспекти безпеки та вимоги до IoT-систем обговорюються в [103]. Обговорення включає життєвий цикл IoT-пристроїв та механізми убезпечення при завантаженні, експлуатації, оновленнях та етапах закінчення терміну функціонування пристроїв. В документі подано опис різних IoT-профілів та розглянуто практичне використання доступних безпекових протоколів на різних етапах життєвого циклу пристроїв. Розглянуто проблеми сучасних протоколів для наскрізної безпеки IoT.

Автори [104] узагальнюють технічні та нетехнічні загрози щодо безпеки IoT-пристроїв та систем. Загрози зібрано на основі практичних відомостей підприємств-виробників IoT-платформ. Безпека та конфіденційність даних вважаються найбільшими викликами, з якими стикаються поточні реалізації IoT-пристроїв та систем.

В проекті [105] розглядаються сучасні мережеві практики захисту IoT-пристроїв. Обговорення включає вимоги щодо безпеки IoT-систем, використання безпекових протоколів та проблеми їх використання. Автори подають рекомендації щодо безпекових рішень та впровадження, корисні для підприємств-виробників IoT-пристроїв. Документ може слугувати орієнтиром для формування мінімальних вимог безпеки IoT-систем слугувати вказівником для вирішення поточних проблем безпеки.

Нові безпекові протоколи обговорюються в [106]. В публікації запропоновано легкий наскрізний ключовий механізм для IoT-пристроїв з обмеженими ресурсами, що використовуються для Інтернеті речей. Цей протокол сформований на основі вивантаження складних обчислювальних криптографічних операцій на сусідній надійний пристрій або вузол з обмеженими ресурсами, що забезпечує функції шифрування та автентифікації. При цьому необхідна наявність довіреної третьої сторони, яка реалізує фунціонал щодо порушення обмежень конфіденційності.

У проекті [107] був запропоновано інформаційно-технологічну архітектуру для задоволення вимог безпеки та конфіденційності протягом життєвого циклу IoT-пристроїв. Сформована архітектура базується на еталонній архітектурній моделі (ARM), розробленій європейським проектом IoT-A розширення взаємодії між IoT-системами. У публікації описано створення, реалізацію, розгортання та тестування запропонованої архітектури IoT-платформах. В [108] подано програмно-алгоритмічне рішення для моніторингу IoT-давачів на базі 6LoWPAN, яке забезпечує відбір даних, ідентифікацію подій, збирання статистичних даних, аналітичне опрацювання та звітування щодо поведінки бездротових давачів. Наявність обширної звітності щодо давачів дозволяє ефективніше виявляти вторгнення та здійснювати глибинну перевірку мережевого IoT-трафіку.

Огляд стандартизованих та нестандартизованих IoT-протоколів подані в роботі [109], а в [110] подано обширний аналіз протоколів та механізмів IoT-безпеки у комплексі з ретельним формуванням питань та проблем.

Автори зосередились на реалізаціях механізмів безпеки та ґенерації ключів і проаналізували ефект їх використання MQTT. Обговорено декілька найсучасніших криптографічних рішень. Описано процедури виявлення вразливостей та ідентифікації вторгнень для IoT-платформ.

3.4 Висновок до третього розділу

В третьому розділі запропоновано девятирівневу архітектуру інформаційно-технологічної платформи для інтеграції та управління IoT-пристроями. При цьому слід відзначити, що безпека все ще залишається однією з найважливіших проблем для IoT-платформ. Тому в розділі подано опис безпекових стандартів, проектів та дослідницьких робіт в галузі Інтернету речей. Описано функції безпеки, реалізовані в IoT-протоколах. Наведено опис та аналіз безпекових стандартів для IoT-платформ, включаючи ACE, TLS/DTLS. Проаналізовано відомості щодо проектів, що обговорюють виклики та загрози безпеці IoT-систем.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Електробезпека робочих місць користувачів комп'ютерів

Інформаційно-технологічна платформа для управління IoT-пристроями формується на основі мережевого, серверного та комп'ютерного обладнання. У всіх розвинених країнах існують сотні документів, які регламентують вимоги не тільки до комп'ютерів, а й до організації робочих місць з їх використанням. Безконтрольне використання комп'ютерної техніки може призвести до негативного впливу на здоров'я користувачів комп'ютерів. Всесвітня організація охорони здоров'я ще в 1989 р. в офсетній публікації № 99 «Відеодисплейні термінали та здоров'я користувачів» дійшла висновку про те, що робота з використанням персональних комп'ютерів супроводжується зоровим і нервово-емоційним напруженням, негативними змінами в кістково-м'язовій системі людини [111].

За способом захисту людини від ураження електричним струмом ВДТ, ЕОМ, периферійні пристрої ЕОМ та обладнання для обслуговування, ремонту і налагодженню ЕОМ мають відповідати 1 класу захисту або бути заземленими відповідно до НПАОП 0.00-1.28-10 [112].

Електромережа живлення має бути трипровідною з фазовим, нульовим робочим і нульовим захисним провідниками, площа перерізу яких має бути не меншою площі перерізу фазового провідника. Нульовий захисний провідник використовують для заземлення електрообладнання, але використовувати, як нульовий робочий його не можна. Підключення нульового робочого і нульового захисного провідників до одного контактного затискача щита живлення заборонено. Усі провідники мають відповідати номінальним параметрам мережі, її навантаженню, умовам навколишнього середовища, температурному режиму, типам апаратури та вимогам ПУЕ.

У приміщенні, де одночасно експлуатують або обслуговують більше п’яти ЕОМ, встановлюють аварійний вимикач, який може вимкнути електроживлення всього приміщення за винятком освітлення. Штепсельні з’єднання й електророзетки мають бути зі спеціальними контактами для підключення нульового захисного провідника. їх конструкція має забезпечити приєднання нульового захисного провідника раніше ніж приєднання фазового та нульового робочого. Порядок їх роз’єднання у разі відключення має бути зворотним. Слід унеможливити з’єднання контактів фазового та нульового захисного провідників. Недопустимим є підключення ЕОМ, периферійних пристроїв ЕОМ і устаткування для обслуговування, ремонту та налагодження ЕОМ до звичайної двопровідної електромережі, в тому числі й з використанням перехідних пристроїв.

Штепсельні з’єднання і електророзетки для напруги у 12 В і 36 В як за своїм кольором, так і за конструкцією мають вирізнятись від штепсельних з’єднань, які розраховані на напругу 127 В і 220 В. Штепсельні з’єднання й електророзетки слід виконувати за магістральною схемою 3...6 з’єднань або електророзеток в одному колі.

Якщо ЕОМ, периферійні пристрої та обладнання розташовують уздовж стін приміщення, то електромережу для їх живлення прокладають підлогою поряд із стінами у металевих трубах і гнучких рукавах відповідно до затвердженого плану. Якщо розташовувати до 5 ЕОМ по периметру приміщення і використовувати при цьому трипровідниковий провід або кабель з негорючого чи важкогорючого матеріалу, дозволяється прокладати електромережу живлення без металевих труб і гнучких металевих рукавів. У разі розташування ЕОМ у центрі приміщення електромережу живлення прокладають під знімною підлогою в металевих трубах і гнучких металевих рукавах, які заземлюють. Заборонено відкрите прокладання кабелів, застосування проводів і кабелів в ізоляції з вулканізованої гуми та інших матеріалів, які містять сірку. Отвори в плитах для прокладання кабелів

електроживлення виконують безпосередньо в місцях встановлення обладнання.

Для підключення переносної електроапаратури застосовують гнучкі проводи в надійній ізоляції. Недопустимими є:

– експлуатація кабелів і проводів з пошкодженою ізоляцією або з такою, що втратила захисні функції, та залишати під напругою кабелі та проводи з неізольованими провідниками;

– застосування саморобних подовжувачів, які не відповідають вимогам ПУЕ до переносних електропроводок;

– застосування для опалення приміщення нестандартного (саморобного) електронагрівального обладнання або ламп розжарювання;

– користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електровиробами, а також лампами, скло яких має сліди затемнення або випинання;

– ідвішування світильників безпосередньо на струмопровідних проводах, обгортання електроламп і світильників папером, тканиною та іншими горючими матеріалами, експлуатація їх із знятими ковпаками (розсіювачами);

– використання електроапаратури та приладів в умовах, то не відповідають рекомендаціям підприємств-виробників.

Живлення комп’ютерів здійснюється віл мережі змінного струму напругою 220 В частотою 50 Гц. Їх підключають до електричної мережі через універсальний адаптер мережі без застосування додаткових трансформаторів або перемикачів па допомогою екранного провідника, який входить до складу комплекту поставки. Вилка провідника може мати 2 або 3 контакти. За допомогою третього контакту підключають додатковий заземлюваний провідник для заземлення комп’ютерів. При цьому заземлені конструкції приміщення (батареї опалення, водопровідні труби, кабелі з заземленим відкритим екраном тощо) надійно захищають діелектричними щитками або сітками від випадкового дотику.

4.2 Організація цивільного захисту на об’єктах промисловості та виконання заходів щодо запобігання виникненню надзвичайних ситуацій техногенного походження

Об’єкт господарської діяльності (підприємство, установа, організація) – основна ланка в системі ЦЗ держави. На об’єкті, де зосереджено людські і матеріальні ресурси, здійснюють економічні і захисні заходи [113]. Відповідно до законодавства, керівництво підприємств, установ і організацій незалежно від форм власності і підпорядкування забезпечує своїх працівників засобами індивідуального та колективного захисту, місцем у захисних спорудах, організовує евакозаходи, створює сили для ліквідації наслідків НС та забезпечує їх готовність, виконує інші заходи з ЦЗ і несе пов’язані з цим матеріальні та фінансові витрати. Власники потенційно небезпечних об’єктів відповідають також за оповіщення і захист населення, що проживає в зонах можливого ураження від наслідків аварій на цих об’єктах [114].

Начальником ЦЗ об’єкта є керівник об’єкта. він відповідає за організацію і стан ЦЗ об’єкта, керує діями органів і сил цз під час проведення рятувальних робіт на ньому. Заступники начальника ЦЗ об’єкта допомагають йому з питань евакуації, матеріально-технічного постачання, інженерно-технічного забезпечення тощо (див. рисунок 4.1). Органом повсякденного управління ЦЗ є відділ (сектор) з питань НС та ЦЗ, який організовує і забезпечує повсякденне керівництво виконанням завдань ЦЗ на об’єкті [115].

Для підготовки та втілення в життя заходів з окремих напрямів створюють служби зв’язку та оповіщення, сховищ і укриттів, протипожежної охорони, охорони громадського порядку, медичної допомоги, протирадіаційного і протихімічного захисту, аварійно-технічного та матеріально-технічного забезпечення тощо. Начальниками служб призначають начальників установ, відділів, лабораторій, на базі яких вони утворюються. Службу зв’язку та оповіщення створюють на базі вузла зв’язку

об’єкта. Головне завдання служби – забезпечити своєчасне оповіщення керівного складу та службовців про загрозу аварії, катастрофи, стихійного лиха, нападу противника; організувати зв’язок і підтримувати його в стані постійної готовності. Протипожежну службу створюють на базі підрозділів відомчої пожежної охорони. Служба розробляє протипожежні профілактичні заходи і контролює їх виконання; організовує локалізацію і гасіння пожежі.

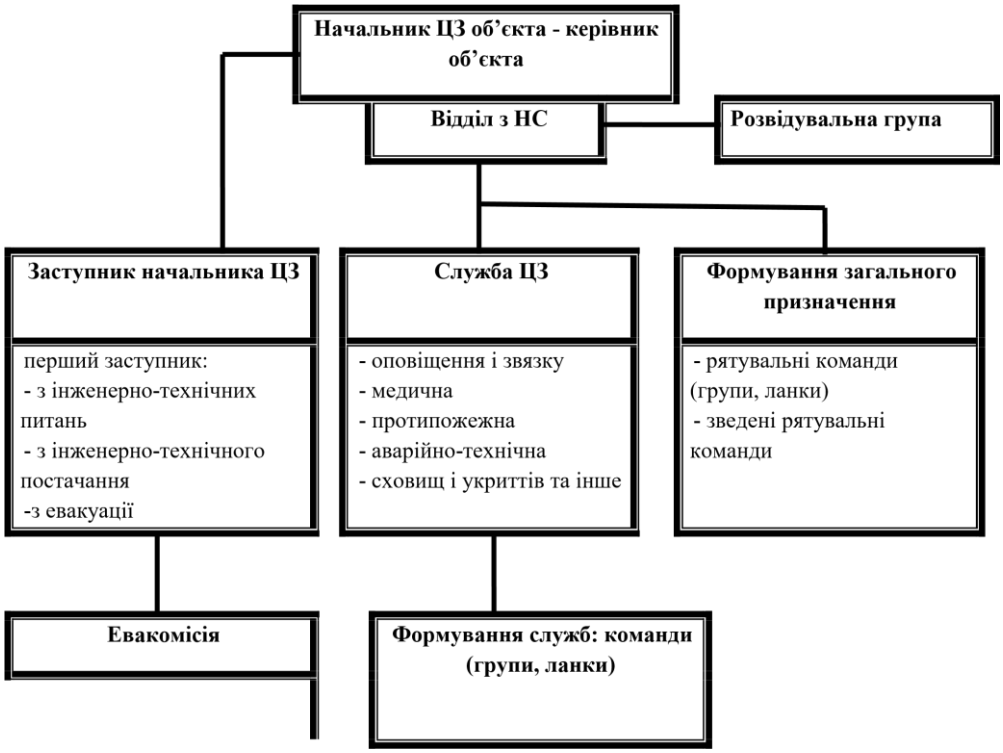

Рисунок 4.1 – Структура ЦЗ об’єкта господарської діяльності

Медичну службу формують на базі медичного пункта, поліклініки об’єкта. На неї покладають організацію проведення санітарно-гігієнічних та профілактичних заходів, надання медичної допомоги потерпілим та евакуацію їх у лікувальні установи, медичне обслуговування робітників, службовців і членів їхніх сімей у місцях розосередження. Службу охорони громадського порядку створюють на базі підрозділів відомчої охорони. Її завдання – організувати і забезпечити надійну охорону об’єкта, громадського порядку в умовах НС, під час ліквідації наслідків аварії, стихійного лиха, а

також у воєнний час. Службу протирадіаційного і протихімічного захисту організовують на базі хімічної лабораторії чи цеху. На неї покладають розробку та здійснення заходів щодо захисту робітників і службовців, джерел водозабезпечення, радіаційного і хімічного спостереження, проведення заходів з ліквідації радіаційного і хімічного зараження та здійснення дозиметричного контролю. Службу сховищ та укриттів організовують на базі відділу капітального будівництва, житлово-комунального відділу. Вона розробляє план захисту робітників, службовців та їх сімей з використанням сховищ та укриттів, забезпечує їх готовність та правильну експлуатацію.

Аварійно-технічну службу створюють на базі виробничо-технічного відділу або відділу головного механіка. Служба розробляє та здійснює попереджувальні заходи, що підвищують стійкість основних споруд, інженерних мереж та комунікацій у НС, організовує проведення робіт з ліквідації і локалізації аварії на комунально-енергетичних мережах.

Службу матеріально-технічного забезпечення створюють на базі відділу матеріально-технічного постачання об’єкта. Вона організовує своєчасне забезпечення формувань усіма засобами оснащення, постачання продуктів харчування і предметів першої необхідності робітників та службовців на об’єкті та у місцях розосередження, ремонт техніки і майна.

Транспортну службу організовують на базі транспортного відділу, гаражу об’єкта. вона розробляє та здійснює заходи із розосередження працівників, забезпечення перевезень, проведення рятувальних робіт тощо.

Кожна служба створює, забезпечує, готує формування служби (команди, групи, ланки) і керує ними під час виконання робіт.

Формування загального призначення – рятувальні загони (команди, групи, ланки), зведені рятувальні загони (команди), підпорядковані безпосередньо начальнику ЦЗ об’єкта. кожне з них має свою структуру і можливості. Наприклад, зведена рятувальна команда (ЗРК) у своєму складі має підрозділи різного призначення, такі як ланка зв’язку і розвідки, дві рятувальні групи, група механізації, санітарна дружина тощо.

ВИСНОВКИ

Завдяки технологічній еволюцію обчислювальних пристроїв, Інтернет речей став життєво важливою частиною сучасного обчислювального світу, особливо для великих обчислювальних інфраструктур. Він має багато програмно-алгоритмічних застосунків у різних сферах. У кваліфікаційній роботі подано аналітичний огляд поточних стандартів і протоколів для Інтернету речей, які розроблені для різних рівнів мережевого стеку.

У першому розділі кваліфікаційної роботи освітнього рівня «Магістр»:

– Описано актуальність досліджень в галузі Інтернету речей.

– Висвітлено проблематику Інтернету речей.

– Проаналізовано сучасний стан досліджень в галузі.

– Описано IoT-екосистему.

У другому розділі кваліфікаційної роботи:

– Розглянуто протоколи передачі даних для IoT-пристроїв та систем.

– Досліджено IoT-протоколи маршрутизації мережевого рівня.

– Описано протоколи інкапсуляції мережевого рівня IoT.

– Проаналізовано IoT-протоколи сеансового рівня.

– Висвітлено протоколи управління IoT-пристроями та системами.

У третьому розділі кваліфікаційної роботи:

– Подано опис сформованої на основі аналізу наукових джерел структури інформаційно-технологічної платформи для інтеграції та управління IoT-пристроями, спроектованої у вигляді девятирівневої моделі.

– На основі опису та анізу запропонованої архітектури зроблено висновок про потребу додаткового опрацювання безпекових засобів для IoT-пристроїв та систем. Тому проаналізовано протоколи та стандарти для їх убезпечення.

– Розглянуто інформаційно-технологічні проєкти для підвищення рівня безпеки IoT-пристроїв.

У розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто електробезпеку робочих місць користувачів комп’ютерів та описано організацію цивільного захисту на об’єктах промисловості та виконання заходів щодо запобігання виникненню надзвичайних ситуацій техногенного походження.

ПЕРЕЛІК ДЖЕРЕЛ

1 Da Xu, Li, Wu He, and Shancang Li. "Internet of things in industries: A survey." *IEEE Transactions on Industrial Informatics* 10.4 (2014): 2233-2243.

2 O. Duda, N. Kunanets, O. Matsiuk, and V. Pasichnyk, "Cloud-based IT Infrastructure for “Smart City” Projects", in *Dependable IoT for Human and Industry: Modeling, Architecting, Implementation*. River Publishers, pp. 389-410, 2018. ISBN: 978-87-7022-013-2.

3 O. Duda, N. Kunanets, O. Matsiuk, and V. Pasichnyk, "Information-Communication Technologies of IoT in the "Smart Cities" Projects", *CEUR Workshop Proceedings*, vol. 2105, pp. 317-330, 2018. ISSN 1613-0073.

4 V. Pasichnyk et al., "Telecommunication Infrastructures for Telemedicine in Smart Cities”, *IDDM 2018 Informatics & Data-Driven Medicine*, vol. 2255, pp. 256-266, 2018. ISSN 1613-0073.

5 Gaikwad, Pranay P., Jyotsna P. Gabhane, and Snehal S. Golait. "A survey based on smart homes system using Internet-of-things." *Computation of Power, Energy Information and Commuincation (ICCPEIC), 2015 International Conference on*. IEEE, 2015.

6 Elmaghraby, Adel S., and Michael M. Losavio. "Cyber security challenges in Smart Cities: Safety, security and privacy." Journal of advanced research 5.4 (2014): 491-497.

7 Bandyopadhyay, Debasis, and Jaydip Sen. "Internet of things: Applications and challenges in technology and standardization." *Wireless Personal Communications* 58.1 (2011): 49-69.

8 Kitchin, Rob. "The real-time city? Big data and smart urbanism." GeoJournal 79.1 (2014): 1-14.

9 Botta, Alessio, et al. "Integration of cloud computing and internet of things: a survey." *Future Generation Computer Systems* 56 (2016): 684-700.

10 D. Tabachyshyn, N. Kunanets, M. Karpinski, O. Duda, and O. Matsiuk, "Information Systems for Processes Maintenance in Socio-communication and

Resource Networks of the Smart Cities", in *Advances in Intelligent Systems and Computing III*, vol. 871, pp 192-205, 2019. ISSN 2194-5365.

11 Mishra, Nilamadhab, Chung-Chih Lin, and Hsien-Tsung Chang. "A cognitive adopted framework for IoT big-data management and knowledge discovery prospective." International Journal of Distributed Sensor Networks 2015 (2015): 6.

12 Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." *IEEE Communications Surveys & Tutorials* 17.4 (2015): 2347-2376.

13 Mantri, Dnyaneshwar S., Neeli Rashmi Prasad, and Ramjee Prasad. "Mobility and Heterogeneity Aware Cluster-Based Data Aggregation for Wireless Sensor Network." Wireless Personal Communications 86.2 (2016): 975-993.

14 A. Kharchenko, et al., "Multicriteria Choice of Software Architecture Using Dynamic Correction of Quality Attributes", *Advances in Computer Science for Engineering and Education II*, vol. 938, 419-427, 2019. ISSN 2194-5365.

15 Li, Fagen, Yanan Han, and Chunhua Jin. "Practical access control for sensor networks in the context of the Internet of Things." Computer Communications (2016).

16 O. Duda, O. Matsiuk, M. Karpinski, N. Veretennikova, N. Kunanets, and V. Pasichnyk, "Information Technologies of Internet Devices and BigData in the “Smart Cities” Projects", in Proc. *13 Intern Scientific and Techn. Conf. on Computer Science and Information Technologies (CSIT)*, vol. 2, Lviv, 2018, pp. 72-75. ISBN: 978-1-5386-6465-0.

17 Bohli, Jens-Matthias, et al. "SMARTIE project: Secure IoT data management for smart cities." *Recent Advances in Internet of Things (RIoT), 2015 International Conference on*. IEEE, 2015.

18 Valera, Antonio J. Jara, Miguel A. Zamora, and Antonio FG Skarmeta. "An architecture based on internet of things to support mobility and security in medical environments." 2010 7th IEEE Consumer Communications and Networking Conference. IEEE, 2010.

19 Vasilomanolakis, Emmanouil, et al. "On the Security and Privacy of Internet of Things Architectures and Systems." 2015 International Workshop on Secure Internet of Things (SIoT). IEEE, 2015.

20 Yang, Jiachen, et al. "Multimedia cloud transmission and storage system based on internet of things." Multimedia Tools and Applications (2015): 1-16.

21 STAMFORD,"Gartner's 2014 hype cycle for emerging technologies maps the journey to digital business," August 2014, http://www.gartner.com/newsroom/id/2819918, (accessed December 04, 2020).

22 Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. McCann, and K. Leung, "A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities," in IEEE Wireless Communications, vol. 20, no. 6, 2013, pp. 91-98.

23 J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the internet of things: A survey of existing protocols and open research issues," in IEEE Communications Surveys Tutorials, vol. 17, no. 3, 2015, pp. 1294-1312.

24 V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," in Transaction on IoT and Cloud Computing, vol. 3, no. 1, 2015, pp. 11-17.

25 A. Al-Fuqaha, M. Guizani, M. Mohaßmmadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols and applications," in IEEE Communications Surveys Tutorials, vol. 17, no. 4, 2015, pp. 2347-2376.

26 Fan, Tongrang, and Yanzhao Chen. "A scheme of data management in the Internet of Things." *2010 2nd IEEE InternationalConference on Network Infrastructure and Digital Content*. IEEE, 2010.

27 Fonseca, Jorge, Carlos Ferraz, and Kiev Gama. "A policy-based coordination architecture for distributed complex event processing in the internet of things: doctoral symposium." *Proceedings of the 10th ACM International Conference on Distributed and Event-based Systems*. ACM, 2016.

28 Khodadadi, Farzad, Rodrigo N. Calheiros, and Rajkumar Buyya. "A data-centric framework for development and deployment of internet of things applications in clouds." *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on*. IEEE, 2015.

29 Xu, Quanqing, et al. "A large-scale object-based active storage platform for data analytics in the internet of things." Advanced Multimedia and Ubiquitous Engineering. Springer Berlin Heidelberg, 2016. 405-413.

30 Kang, Jun, Siqing Yin, and Wenjun Meng. "An Intelligent Storage Management System Based on Cloud Computing and Internet of Things." Proceedings of International Conference on Computer Science and Information Technology. Springer India, 2014.

31 Busold, Christoph, et al. "Smart and Secure Cross-Device Apps for the Internet of Advanced Things." International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2015.

32 Jin, Jiong, et al. "An information framework for creating a smart city through internet of things." *IEEE Internet of Things Journal* 1.2 (2014): 112-121.

33 Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things." Computer Networks 57.10 (2013): 2266-2279.

34 Sicari, Sabrina, et al. "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks 76 (2015): 146-164.

35 Salman, Tara, and Raj Jain. "A survey of protocols and standards for internet of things." *arXiv preprint arXiv:1903.11549* (2019).

36 IEEE802.15.4-2011, “IEEE standard for local and metropolitan area network–part 15.4: Low-rate wireless personal area networks (LR-WPAN),” in IEEE Standards, April, 2012, pp.1-225.

37 M. Park, “IEEE 802.11ah: sub-1-ghz license-exempt operation for the internet of things,” IEEE Communications Magazine, vol. 53, no. 9, 2015, pp. 145-151.

38 M. Nobre, I. Silva, and L. A. Guedes, "Routing and scheduling algorithms for WirelessHART Networks: a survey," in Sensors 15, no. 5, 2015, pp. 9703-9740.

39 Z-Wave, “Z-wave protocol overview,” April 2006, https://wiki.ase.tut.fi/courseWiki/images/9/94/SDS10243_2_Z_Wave_Protocol_Overview.pdf, (accessed December 04, 2020).

40 J. Decuir, “Bluetooth 4.0: Low Energy,” 2010, https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205Decuir.pdf , (accessed December 04, 2020).

41 Zigbee, “Zigbee resource guide,” 2016, http://www.nxtbook.com/nxtbooks/webcom/zigbee_rg2016/#/0, (accessed December 04, 2020).

42 O. Cetinkaya and O. Akan, “A dash7-based power metering system,” in 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), 2015, pp. 406–411.

43 HomePlog Alliance, “HomePlug™ AV2 Technology,” 2007 http://www.homeplug.org/media/filer_public/2c/32/2c327fc8-25bb409e-abf7-c398534c24dc/homeplug_av2_whitepaper_130909.pdf , (accessed December 04, 2020).

44 M. Hasan, E. Hossain, and D. Niyato, “Random access for machine- to-machine communication in lte-advanced networks: issues and approaches,” in IEEE Communications Magazine, vol. 51, no. 6, 2013, pp. 86-93.

45 J. Lee, Y. Kim, Y. Kwak, J. Zhang, A. Papasakellariou, T. Novlan, C. Sun and Y. Li, "LTE-advanced in 3GPP Rel -13/14: an evolution toward 5G," in IEEE Communications Magazine, vol. 54, no. 3, 2016, pp. 36-42.

46 C. Hoymann, D. Astely, M. Stattin, G. Wikstrom, J. F. Cheng, A. Hoglund, M. Frenne, R. Blasco, J. Huschke and F. Gunnarsson, "LTE release 14 outlook," in *IEEE Communications Magazine,* vol. 54, no. 6, 2016, pp. 44-49.

47 N. Sornin, M. Luis, T. Eirich, T. Kramp, and O.Hersent, “Lorawan specification,” LoRa Alliance, January 2015,

https://www.loraalliance.org/portals/0/specs/LoRaWAN%20Specification%201R0.pdf, (accessed December 04, 2020).

48 I. Poole, “Weightless wireless — m2m white space communications-tutorial,” 2014, http://www.radioelectronics.com/info/wireless/weightless-m2m-white-space-wireless-communications/basics-overview.php, (accessed December 04, 2020).

49 S. Bush, “Dect/ule connects homes for iot,” September 2015, http://www.electronicsweekly.com/news/design/communications/dect-ule-connects-homes-iot-2015-09/, (accessed December 04, 2020).

50 EnOcean, “EnOcean – The World of Energy Harvesting Wireless Technology,” 2015, https://www.enocean.com/en/technology/white-papers/, (accessed December 04, 2020).

51 R. Kshetrimayum, “An introduction to uwb communication systems,” in IEEE Potentials, vol. 28, no. 2, 2013, pp. 9-13.

52 S. Evanczuk, “ANT/ANT+ Solutions Speed Low-Power Wireless Design,” February 2013, http://www.digikey.com/en/articles/techzone/2013/feb/antant-solutions-speed-lowpower-wireless-design, (accessed December 04, 2020).

53 ISA, “Isa100.11a technology standard,” 2009, http://www.nivis.com/technology/ISA100.11a.php, (accessed December 04, 2020).

54 T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” IETF RFC 6550, March 2012, http://www.ietf.org/rfc/rfc6550.txt, (accessed December 04, 2020).

55 Aijaz and A. Aghvami, “Cognitive machine-to-machine communications for internet-of-things: A protocol stack perspective,” in IEEE Internet of Things Journal, vol. 2, no. 2, 2015, pp. 103-112.

56 S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini, “Carp: A channel-aware routing protocol for underwater acoustic wireless networks,” in Ad Hoc Networks, vol. 34, 2015, pp. 92-104.

57 D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, “6tisch: deterministic ip-enabled industrial internet of things,” in IEEE Communications Magazine, vol. 52, no. 12, 2014, pp. 36–41.

58 Internet Engineering Task Force, “IPv6 over Networks of Resource-constrained Nodes (6lo),” https://datatracker.ietf.org/wg/6lo/documents/, (accessed December 04, 2020).

59 J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby ,and C. Gomez, “IPv6 over BLUETOOTH(R) Low Energy,” IETF RFC 7668, October 2015, http://www.ietf.org/rfc/rfc7668.txt, (accessed December 04, 2020).

60 OASIS, “MQTT Version 3.1.1,” 2014, http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf, (accessed December 04, 2020).

61 M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, “Secure mqtt for internet of things (iot),” in Fifth International Conference on Communication Systems and Network Technologies (CSNT), 2015, pp. 746-751.

62 OASIS, “Oasis advanced message queuing protocol (amqp) version 1.0,” 2012, from http://docs.oasisopen.org/amqp/core/v1.0/os/amqp-core-complete-v1.0-os.pdf, (accessed December 04, 2020).

63 Z. Shelby, K. Hartke, and C. Bormann, “The Constrained Application Protocol (CoAP),” IETF RFC 7252, June 2014, http://www.ietf.org/rfc/rfc7252.txt, (accessed December 04, 2020).

64 P. Saint-Andre, “Extensible Messaging and Presence Protocol (XMPP): Core,” IETF RFC 6120, March 2011 https://tools.ietf.org/html/rfc6120, (accessed December 04, 2020).

65 O. M. Group, “Data Distribution Service (DDS)-v1.4,” April 2015, http://www.omg.org/spec/DDS/1.4, (accessed December 04, 2020).

66 IEEE, “IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies," in IEEE Standards 1905.12013, 2013, pp.1-93.

67 K. Malar and N. Kamaraj, “Development of smart transducers with ieee 1451.4 standard for industrial automation,” in International Conference on

Advanced Communication Control and Computing Technologies (ICACCCT), 2014, pp. 111-114.

68 A. John Blackford, and P. Mike Digdon, “Tr-069 CPE wan management protocol,” 2013, https://www.broadbandforum.org/technical/download/TR-069.pdf, (accessed December 04, 2020).

69 Open Mobile Alliance, “Device Management Architecture,” 2016, http://www.openmobilealliance.org/release/DM/V2_020160209-A/OMA-AD-DM-V2_0-20160209-A.pdf, (accessed December 04, 2020).

70 Open Mobile Alliance, “Lightweight machine to machine architecture,” December 2013, http://www.openmobilealliance.org/release/LightweightM2M/V1_0-20151214-C/OMA-AD-LightweightM2M-V1_0-20131210C.pdf, (accessed December 04, 2020).

71 O. Duda, V. Kochan, N. Kunanets, O. Matsiuk, V. Pasichnyk, and A. Sachenko, "Data Processing in IoT for Smart City Systems", in *Proc. 10th IEEE Intern. Conf. on. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2019),* Metz, 2019. pp. 96-99.

72 Abbasi, Mohammad Asad, et al. "Addressing the future data management challenges in iot: A proposed framework." *International Journal of Advanced Computer Science and Applications* 8.5 (2017): 197-207.

73 Jin, Jiong, et al. "An information framework for creating a smart city through internet of things." *IEEE Internet of Things Journal* 1.2 (2014): 112-121.

74 Ваник А.Г., Притоцький О.О., Яєчник О.П., Маєвський Т.О., Використання IoT-пристроїв для відбору біомедичних даних в умовах пандемії COVID-19, Матеріали VIII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 9 – 19грудня 2020р.). – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2020. – С.83.

75 Bonomi, Flavio, et al. "Fog computing and its role in the internet of things." *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. ACM, 20126.

76 Qaisar, Saad, and Nida Riaz. *Fog Networking: An Enabler for Next Generation Internet of Things*. International Conference on Computational Science and Its Applications. Springer International Publishing, 2016.

77 Bowers, Kevin D., Ari Juels, and Alina Oprea. "HAIL: a high-availability and integrity layer for cloud storage." Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009.

78 Mishra, Nilamadhab, Chung-Chih Lin, and Hsien-Tsung Chang. "A cognitive adopted framework for IoT big-data management and knowledge discovery prospective." International Journal of Distributed Sensor Networks 2015 (2015): 6.

79 Ваник А.Г., Гніздюх В.Г., Яєчник О.П., Маєвський Т.О., Аналітичне опрацювання відомостей щодо COVID-19, Матеріали VIII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 9 – 19грудня 2020р.). – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2020. – С.82.

80 Babar, Sachin, et al. "Proposed embedded security framework for internet of things (iot)." Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on. IEEE, 2011.

81 Tan, Lu, and Neng Wang. "Future internet: The internet of things." *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*. Vol. 5. IEEE, 2010.

82 G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks,” IETF RFC 4944, September 2007, https://tools.ietf.org/html/rfc4944 (accessed December 04, 2020).

83 J. Hui and P. Thubert, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, IETF RFC 6262, September 2011, https://tools.ietf.org/html/rfc6282 (accessed December 04, 2020).

84 E. Kim, D. Kaspar, and J. Vasseur, “Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs),” IETF RFC 6568, April 2012, http://www.ietf.org/rfc/rfc6568.txt (accessed December 04, 2020).

85 Internet Engineering Task Force, “IPv6 over Networks of Resource-constrained Nodes (6lo),” https://datatracker.ietf.org/wg/6lo/documents/, (accessed December 04, 2020).

86 P. Pongle and G. Chavan, “A Survey: Attacks RPL and 6LowPAN in IoT,” in International Conference on Pervasive Computing (ICPC 2015), Pune, India, 2015, pp. 1-6.

87 A. Roger, T. Tsao, V. Daza, A. Lozano, M. Richardson, and M. Dohler, "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)," IETF RFC 7416, January 2015, https://tools.ietf.org/html/rfc7416 (accessed December 04, 2020).

88 H. Tschofenig, and T. Fossati,“Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things,” IETF RFC 7925, July 2016, https://tools.ietf.org/html/rfc7925 (accessed December 04, 2020).

89 IEEE1888, “IEEE standard for ubiquitous green community control network: Security,” in IEEE Standards 1888.3-2013, 2013, pp. 1-30.

90 TCG, “Guidance for securing iot using tcg technology,” September 2015, http://www.trustedcomputinggroup.org/guidancesecuring-iot-using-tcg-technology-reference-document/ (accessed December 04, 2020).

91 D. Hardt, “The OAuth 2.0 Authorization Framework,” IETF RFC 6749, October 2012, http://www.ietf.org/rfc/rfc6749.txt (accessed December 04, 2020).

92 L. Torsten, M. McGloin, and P. Hunt. “OAuth 2.0 threat model and security considerations,” IETF RFC 6819, January 2013, http://www.ietf.org/rfc/rfc6819.txt (accessed December 04, 2020).

93 T. Lodderstedt, J. Bradley, and A. Labunets, “OAuth Security Topics,” IETF Draft Nov, 2016. https://tools.ietf.org/html/draftlodderstedt-oauth-security-topics-00 (accessed December 04, 2020).

94 A. Melnikov and K. Zeilenga, “Simple Authentication and Security Layer (SASL),” IETF RFC 4422, June 2006, http://www.ietf.org/rfc/ rfc4422.txt (accessed December 04, 2020).

95 L. Seitz, S. Gerdes, G. Selander, M. Mani, and S. Kumar, “Use Cases for Authentication and Authorization in Constrained Environments,” IETF RFC 7744 Jan. 2016, http://www.ietf.org/rfc/rfc7744.txt (accessed December 04, 2020).

96 S. Gerdes, L. Seitz, S. Gerdes, and G. Selander, “An architecture for authorization in constrained environments,” IETF Draft, August 2016, https://www.ietf.org/id/draft-ietf-ace-actors-04.txt (accessed December 04, 2020).

97 Wikipedia, “Blockchain (database),” https://en.wikipedia.org/wiki/ Blockchain_(database), (accessed December 04, 2020).

98 Postscapes, “Blockchain IoT Projects and Applications | 2016 Guide,” http://www.postscapes.com/blockchains-and-the-internetof-things/ (accessed December 04, 2020).

99 P. Kianmajd, J. Rowe and K. Levitt, "Privacy-preserving coordination for smart communities," in IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 1045-1046.

100 S. H. Hashemi, F. Faghri, P. Rausch and R. H. Campbell, "World of Empowered IoT Users," in IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), 2016, pp. 13-24.

101 K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, 2016, pp. 2292-2303.

102 A. Marcella, “Blockchain-Based Architectures for the Internet of Things: A Survey,” May 15, 2016, https://ssrn.com/abstract=2846810, (accessed December 04, 2020).

103 O. Garcia-Morchon, S. Kumar and M. Sethi, “Security Considerations in the IP-based Internet of Things,” IETF Draft, Feb. 2017, Available: https://www.ietf.org/id/draft-irtf-t2trg-iot-seccons-01.txt (accessed December 04, 2020).

104 H. Baba, Y. Ishida, T. Amatsu, K. Maeda, “Problems in and among industries for the prompt realization of IoT and safety considerations,” IETF Draft, Oct. 2016, https://datatracker.ietf.org/doc/draft-baba-iot-problems/ (accessed December 04, 2020).

105 K. Moore, R. Barnes, H. Tschofenig, “Best Current Practices for Securing Internet of Things (IoT) Devices,” IETF Draft, Oct. 2016, https://tools.ietf.org/html/draft-moore-iot-security-bcp-00 (accessed December 04, 2020).

106 M. A. Iqbal and M. Bayoumi, "Secure End-to-End key establishment protocol for resource-constrained healthcare sensors in the context of IoT," 2016 International Conference on High Performance Computing & Simulation (HPCS), 2016, pp. 523-530.

107 J. L. Hernandez-Ramos, J. B. Bernabe and A. Skarmeta, "ARMY: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things," in IEEE Communications Magazine, vol. 54, no. 9, 2016, pp. 28-35.

108 V. H. La, R. Fuentes and A. R. Cavalli, "A novel monitoring solution for 6LoWPAN-based Wireless Sensor Networks," in 22nd Asia-Pacific Conference on Communications (APCC), 2016, pp. 230-237.

109 S. A. Kumar, T. Vealey and H. Srivastava, "Security in Internet of Things: Challenges, Solutions and Future Directions," in 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 5772-5781.

110 S. Zamfir, T. Balan, I. Iliescu and F. Sandu, "A security analysis on standard IoT protocols," in International Conference on Applied and Theoretical Electricity (ICATE), 2016, pp. 1-6.

111 Охорона праці при роботі з комп'ютерною технікою, https://oppb.com.ua/content/ohorona-praci-pry-roboti-z-kompyuternoyu-tehnikoyu (accessed December 04, 2020).

112 НПАОП 0.00-1.28-10. Про затвердження правил охорони праці під час експлуатації електронно-обчислювальних машин (31562), https://dnaop.com/html/31562/doc-%D0%9D%D0%9F%D0%90%D0%9E%D0%9F_0.00-1.28-10 (accessed December 04, 2020).

113 Кулаков, Микола Анатолійович, et al. "Цивільна оборона." (2005).

114 Стручок, Володимир Сергійович, Олена Степанівна Стручок, and Дарія Володимирівна Мудра. "Навчальний посібник до написання розділу дипломного проекту та дипломної роботи ″Безпека в надзвичайних ситуаціях ″для студентів всіх спец. денної, заочної (дистанційної) та екстернатної форм навчання." (2017).

115 Корецький, Ю. О. "МЕХАНІЗМИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ БЕЗПЕКИ ПРИ НАДЗВИЧАЙНИХ СИТУАЦІЯХ." *РЕДАКЦІЙНА КОЛЕГІЯ: ТИЩЕНКО Олександр–заступник начальника ЧІПБ імені Героїв Чорнобиля НУЦЗ України з навчальної та наукової роботи, кандидат технічних наук, професор, заслужений працівник освіти України*.

ДОДАТКИ

Додаток А

Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

VIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

9–10 грудня 2020 року

ТЕРНОПІЛЬ
2020

УДК 004.62
Ваник А.Г., Гніздюх В.Г., Яєчник О.П., Маєвський Т.О.
(Тернопільський національний технічний університет імені Івана Пулюя)

АНАЛІТИЧНЕ ОПРАЦЮВАННЯ ВІДОМОСТЕЙ ЩОДО COVID-19

UDC 004.62
Vanyk A.H., Hnizdiukh V.H., Yaiechnyk O.P., Maievskyi T.O.

ANALYTICAL PROCESSING OF COVID-19 INFORMATION

Глобальна пандемія Covid-19 вимагає комплексної та глобальної реакції всіх світових та національних медичних організацій та установ, що функціонують в галузі охорони здоров'я. Covid-19 спричинив загострення проблем в галузі охорони здоров'я та виявив необхідність безперешкодного, швидкого та своєчасного обміну даними щодо глобальних пандемій та підвищив вимоги щодо оперативного реагування [1]. Оскільки COVID-19 швидко поширився по всьому світу, ефективне використання моделей прогнозування може відіграти визначну роль для допомоги в управлінні ресурсами охорони здоров'я та плануванні профілактичних заходів.

Алгоритми та методи аналітичного опрацювання даних – це добре відомі інструменти та засоби для розроблення прогнозних моделей та практичного аналізу даних. З їх використанням можна видобувати приховану або неявно подану корисну інформацію з наборів та колекцій необроблених даних [2]. Видобуті знання та відомості щодо глобальної пандемії COVID-19 можуть бути використані не тільки в галузі охорони здоров'я а й у різних сферах. На даний час в галузі охорони здоров'я створено та продовжується накопичення великої кількості даних щодо COVID-19, включаючи дані про пацієнтів, супутні захворювання та діагнози.

В інтелектуальному аналізі відомостей щодо COVID-19, виділяють дві категорії завдань. Перша категорія – це описові завдання, що стосуються загальних властивостей даних про COVID-19. Дріга категорія – це передбачувальні (прогнозні) завдання, основною метою яких є побудова моделей, що можуть оцінити відображення корисних знань від інформаційних входів до виходів за допомогою навчальної вибірки даних. Навчені моделі можуть бути використані для прогнозування результатів для наборів вхідних відомостей щодо COVID-19. У порівнянні з традиційним статистичним аналізом, методи, що відносяться до другої категорії будуть більш гнучкими та ефективними в задачах дослідницького аналізу [3].

Це лише початок наукових досліджень щодо аналітичного опрацювання відомостей, зібраних про COVID-19 з різнотипових джерел. Незважаючи на те, що сформовані на даний час прогнозні моделі не дуже точні [2], вони можуть бути корисними для побудови точних моделей на основі більшої агрегації даних щодо COVID-19. Відставання у прогнозуванні може бути наслідком неоднозначності захворюваності в різних країнах. Подальші дослідження потребують поглибленого аналізу доступних наукових джерел.

Література.

1. Radanliev, Petar, David De Roure, and Rob Walton. "Data mining and analysis of scientific research data records on Covid-19 mortality, immunity, and vaccine development-In the first wave of the Covid-19 pandemic." Diabetes & Metabolic Syndrome: Clinical Research & Reviews 14.5 (2020): 1121-1132.
2. Ayyoubzadeh, Seyed Mohammad, et al. "Predicting COVID-19 incidence through analysis of google trends data in iran: data mining and deep learning pilot study." JMIR Public Health and Surveillance 6.2 (2020): e18828.
3. Sherstinsky, Alex. "Fundamentals of recurrent neural network (rnn) and long short-term memory (lstm) network." Physica D: Nonlinear Phenomena 404 (2020): 132306.

УДК 004.67

Ваник А.Г., Притоцький О.О., Яєчник О.П., Маєвський Т.О.
(Тернопільський національний технічний університет імені Івана Пулюя)

ВИКОРИСТАННЯ ІОТ-ПРИСТРОЇВ ДЛЯ ВІДБОРУ БІОМЕДИЧНИХ ДАНИХ В УМОВАХ ПАНДЕМІЇ COVID-19

UDC 004.67

Vanyk A.H., Prytotskyi O.O., Yaiechnyk O.P., Maievskyi T.O.

USE OF IOT DEVICES FOR BIOMEDICAL DATA SELECTION IN A COVID-19 PANDEMIC

Повідомляється, що в світі до завершення 2020 року буде підключено понад 50 мільярдів пристроїв з використанням засобів радіозв'язоку [1]. На їх основі формуються IoT-мережі давачів, мобільних пристроїв, радіоідентифікаційних міток та виконавчих пристроїв, котрі запрограмовані на збирання даних із середовища користувача. IoT-мережі ефективно використовуються у багатьох галузях, зокрема в системі охорони здоров'я, управліні процесами постачання енергоносіїв та комунальних послуг, розумних будинках, безпекових системах та сільському господарстві. Функціональні можливості IoT-пристроїв при комплексному використання з «розумними» інформаційними технологіями суттєво розширюють можливості надання високоякісних та своєчасних послуг в умовах глобальної пандемії COVID-19. Послуги сформовані на базі IoT-пристроїв із залученням смартфонів стали інноваційною мережевою парадигмою яка консолідує розподілені послуги та фізичні об'єкти.

В роботі [2] подано опис системи виявлення та моніторингу COVID-19 у режимі реального часу. Запропонована авторами система використовує інформаційно-технологічний концепт Інтернету речей (IoT) для відбору відомостей щодо симптомів COVID-19, раннього виявлення підозр захворювання, моніторингу реакції на лікування інфікованих громадян, постлікувального спостереження пацієнтів та розширення розуміння природи захворювання. В [3] Ндіає описує вплив глобальної пандемії COVID-19, на розвиток інформаційних та комунікаційних технологій, зокрема IoT. Він розглядає внесок IoT та пов'язаних з ними сенсорних технологій у процеси відстеження вірусів та пом'якшення наслідків. В публікації розглядаються супутні проблеми розгортання апаратного забезпечення давачів в умовах швидко поширюваної пандемії. Сінх [4] досліджує загальне застосування IoT, пропонуючи перспективну дорожню карту для подолання пандемії COVID-19. Автор аналізує дванадцять програм для IoT-притроїв.

Очікується, що світові потрібно буде боротися з пандемією COVID-19 з використанням обережних заходів, поки не буде розроблена дієва вакцина. Тому формування ефективних інформаційно-технологічних систем для відбору біомедичних даних з використанням IoT-пристроїв в умовах пандемії COVID-19 є актуальним напрямком досліджень та потребує детальнішого опрацювання.

Література.

1. Kolhar, Manjur, et al. "A three layered decentralized IoT biometric architecture for city lockdown during COVID-19 outbreak." IEEE Access 8 (2020): 163608-163617.
2. Otoom, Mwaffaq, et al. "An IoT-based framework for early identification and monitoring of COVID-19 cases." Biomedical Signal Processing and Control 62 (2020): 102149.
3. Ndiaye, Musa, et al. "IoT in the Wake of COVID-19: A Survey on Contributions, Challenges and Evolution." IEEE Access 8 (2020): 186821-186839.
4. Singh, Ravi Pratap, et al. "Internet of things (IoT) applications to fight against COVID-19 pandemic." Diabetes & Metabolic Syndrome: Clinical Research & Reviews (2020).