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

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

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Аналіз безпеки периферійних обчисленнь з мультидоступом в мережах 5G

Виконав: студент IV курсу, групи СБзс-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Ніколаєва Х.Я. (прізвище та ініціали)

Керівник (підпис) Дуда О.М. (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т.Б. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) Дячук С.Ф. (прізвище та ініціали)

Тернопіль
2022

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

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

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«_16_» _червня_ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Ніколаєвій Христині Ярославівні
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз безпеки периферійних обчисленнь з мультидоступом в мережах 5G

Керівник роботи Дуда О.М., к.т.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «23» березня 2022 року № 4/7-177

2. Термін подання студентом завершеної роботи 16 червня 2022р.

3. Вихідні дані до роботи Наукові публікації про периферійні обчислення з мультидоступом та безпекові особливості їх використання в мережах 5G

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз предметної області та категорії застосунків. 1.1 Периферійні обчислення з мультидоступом в мережах 5G. Стан та перспективи досліджень. 1.2 Категорії застосунків що використовують периферійні обчислення з мультидоступом в мережах 5G. 1.3. Висновок до першого розділу. 2. Аналіз безпеки периферійних обчислень з мультидоступом в мережах 5G. 2.1 Уразливості безпеки та існуючі рішення для захисту периферійних обчислень з мультидоступом в мережах 5G. 2.2 Результати аналізу вразливостей безпеки. 2.3 Результати аналізу існуючих рішень щодо запобігання та протидії вразливостям безпеки. 2.4 Безпекові проблеми та перспективи подальших досліджень для широкої адаптації периферійних обчислень з мультидоступом в 5G-мережах. 2.5 Висновок до другого розділу.
3. Безпека життєдіяльності, основи охорони праці. 3.1 Шляхи підвищення життєдіяльності людини. 3.2 Організація ведення робіт в аварійних умовах. 3.3 Висновок до третього розділу.
Висновки. Перелік джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Титульна сторінка. 2 Тема та мета роботи. 3 Завдання роботи. 4 Актуальність роботи. 5. Мобільна технологія п'ятого покоління (5G). 6. Edge Computing. 7. Структура та функціонування. 8. Використання периферійних обчислень з мультидоступом. 9. Безпекові загрози при підключенні критичної інфраструктури. 10. Безпекові проблеми, пов'язані з використанням апаратних платформ. 11. Безпекові проблеми по категоріях використання. 12. Методи виявлення аномалій. 13. Безпекові архітектури та структури. 14. Висновки. 14. Висновки. 15 Завершальний слайд.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Гурик О.Я., доцент кафедри МТ	04.04.2022	01.05.2022

7. Дата видачі завдання 24 січня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.01.2022	*Виконано*
2.	Підбір джерел про периферійні обчислення з	04.01.2022-30.01.2022	*Виконано*
	мультидоступом та безпекові особливості їх		
	використання в мережах 5G		
3.	Переклад та опрацювання джерел про периферійні	31.01.2022-06.02.2022	*Виконано*
	обчислення з мультидоступом та безпекові		
	особливості їх використання в мережах 5G		
4.	Виконання дослідження щодо безпеки периферійних	07.02.2022-13.02.2022	*Виконано*
	обчислень з мультидоступом в мережах 5G		
5.	Оформлення розділу «Аналіз предметної області та	14.02.2022-06.03.2022	*Виконано*
	категорії застосунків»		
6.	Оформлення розділу «Аналіз безпеки периферійних	07.03.2022-03.04.2022	*Виконано*
	обчислень з мультидоступом в мережах 5G»		
7.	Виконання завдання до підрозділу «Безпека життєдіяльності»	04.04.2022-17.04.2022	*Виконано*
8.	Виконання завдання до підрозділу «Основи охорони	18.04.2022-01.05.2022	*Виконано*
	праці»		
9.	Оформлення кваліфікаційної роботи	02.05.2022-15.05.2022	*Виконано*
10.	Нормоконтроль	16.05.2022-22.05.2022	*Виконано*
11.	Перевірка на плагіат	03.06.2022	*Виконано*
12.	Попередній захист кваліфікаційної роботи	06.06.2022	*Виконано*
13.	Захист кваліфікаційної роботи	17.06.2022	

Студент _____ Ніколаєва Х.Я.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Дуда О.М.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз безпеки периферійних обчисленнь з мультидоступом в мережах 5G // Кваліфікаційна робота освітнього рівня «Бакалавр» // Ніколаєва Христина Ярославівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБзс-41 // Тернопіль, 2022 // С. 53, рис. – 9, табл. – 6, кресл. – 15, бібліогр. – 72.

Ключові слова: 5G, безпека, захист, запобігання, мережа, мультидоступ, периферійні обчислення.

Кваліфікаційна робота присвячена аналізу безпеки периферійних обчисленнь з мультидоступом в мережах 5G.

Мета роботи – підвищення рівня поінформованості про безпекові загрози у різних галузях використання периферійних обчислень з мультидоступом в мережах 5G

В першому розділі кваліфікаційної роботи освітнього рівня «Бакалавр» проведено аналіз предметної області та категорій застосунків. Зафіксовано стан та перспективи досліджень в галузі. Описано безпекові загрози та ризики інноваційних мереж 5G. Проаналізовано безпекові загрози та ризики периферійних обчисленнь з мультидоступом. Розглянуто категорії застосунків що використовують периферійні обчислення з мультидоступом в мережах 5G.

В другому розділі кваліфікаційної роботи проведено аналіз безпеки периферійних обчислень з мультидоступом в мережах 5G. Досліджено уразливості безпеки та існуючі рішення для захисту периферійних обчислень з мультидоступом в мережах 5G. Подано результати аналізу вразливостей безпеки. Висвітлено результати аналізу існуючих рішень щодо запобігання та протидії вразливостям безпеки. Описано безпекові проблеми та перспективи подальших досліджень.

ANNOTATION

Analysis of peripheral calculations safety with multiaccess in 5G networks // Qualification work of educational level "Bachelor" // Nikolaieva Khrystyna Yaroslavivna // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, group SBzs-41 // Ternopil, 2022 // P. 53, fig. - 9, tables - 6, chair.- 15, ref. - 72.

Keywords: 5G, security, protection, prevention, network, multi access, peripheral computing.

Qualification work is devoted to the analysis of the security of peripheral computing with multi-access in 5G networks.

The aim of the work is to raise awareness about security threats in various areas of the use of peripherals with multi-access in 5G networks

In the first section of the qualification work of the educational level "Bachelor" the analysis of the subject area and categories of applications is carried out. The state and prospects of research in the field are recorded. The security threats and risks of 5G innovation networks are described. Security threats and risks of peripheral calculations with multi-access are analyzed. Categories of applications using peripheral computing with multi-access in 5G networks are considered.

The second section of the qualification work analyzes the security of peripheral computing with multi-access in 5G networks. Security vulnerabilities and existing solutions for the protection of peripheral computing with multi-access in 5G networks have been studied. The results of the analysis of security vulnerabilities are presented. The results of the analysis of existing solutions to prevent and combat security vulnerabilities are highlighted. Security issues and prospects for further research are described.

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ

БПЛА – Безпілотні літальні апарати.

AR (англ. Augmented Reality) – Доповнена реальність.

CDN (англ. Content Delivery Network або Content Distribution Network) – мережа доправлення (і розповсюдження) контенту.

FC (англ. Fog computing) – Туманні обчислення.

EC (англ. Edge Computing) – Граничні обчислення.

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

M2M (англ. Machine-to-Machine) – Міжмашина взаємодія.

MIMO (англ. Multiple Input Multiple Output) – Множинні вводи та виходи.

MNO (англ. Mobile Network Operator) – Оператор мобільної мережі.

MR (англ. Mixed Reality) – Змішана реальність.

TC (англ. Transparent Computing) – Прозорі обчислення.

QoS (англ. Quality of Service) – Якість послуг (якість обслуговування).

QoE (англ. Quality of Experience) – Якість досвіду.

VR (англ. Virtual reality) – віртуальна реальність.

V2E (англ. Vehicle-to-Everything) – Транспортний засіб до всього.

V2I (англ. Vehicle-to-Infrastructure) – Транспортний засіб до інфраструктури.

V2N (англ. Vehicle-to-Network) – Транспортний засіб до мережі.

VN (англ. Vehicle Network) – Мережа транспортних засобів.

ЗМІСТ

ВСТУП

Актуальність теми. Перспективи розвитку мобільних та інтернет-технологій декларують досягнення за межами сучасної науки. Концепції автоматизованого водіння, доповненої реальності та міжмашинної комунікації є доволі складними по своїй суті та потребують збільшення обчислювальних потужностей та функціональних можливостей мобільної інфраструктури. Мобільні мережі 5G дозволяють забезпечити обслуговування комунікаційних та обчислювальних потреб інноваційних інформаційних технологій, але на даний час їм бракує розвинутої кінцевої мережевої інфраструктури. Пограничні обчислення з багатьма доступом (MEC) можуть забезпечити таку периферійну інформаційно-технологічну платформу. Тому актуальним є аналіз вразливостей безпеки ключових випадків використання периферійних обчислень з мультидоступом на основі 5G. Доцільно виокремити та проаналізувати ймовірні загрози безпеки дл кожного випадку їх практичного використання, а також запропонувати контрзаходи для їх пом’якшення.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Бакалавр» є підвищення рівня поінформованості про безпекові загрози у різних галузях використання периферійних обчислень з мультидоступом в мережах 5G. Для досягнення мети потрібно:

– Проаналізувати стан досліджень щодо вразливостей безпеки периферійних обчислень з мультидоступом в мережах 5G.

– Виокремити та описати категорії застосунків що використовують периферійні обчислення з мультидоступом в мережах 5G.

– Проаналізувати вразливості безпеки периферійних обчислень з мультидоступом в мережах 5G.

– Проаналізувати існуючі рішення для захисту периферійних обчислень з мультидоступом в мережах 5G.

– Описати безпекові проблеми та перспективи подальших досліджень для широкої адаптації периферійних обчислень з мультидоступом в 5G-мережах.

Практичне значення одержаних результатів. На основі проведеного аналізу наукових літературних джерел сформовано опис пов’язаних з використанням апаратних платформ периферійних обчислень з мультидоступом в мережах 5G безпекових проблем.

Узагальнюючи аналіз наукових літературних джерел, сформовано опис безпекових проблеми по категоріях використання периферійних обчислень з мультидоступом в мережах 5G.

На основі проведеного аналізу наукових літературних джерел сформовано перелік криптографічних, Блокчейн-методів, методів виявлення аномалій, інформаційно-технологічних архітектур та структур для підвищення рівня безпеки та контрзаходів безпеки при використанні периферійних обчислень з мультидоступом в мережах 5G

Подано опис безпекові проблем та перспективи подальших досліджень для широкої адаптації периферійних обчислень з мультидоступом в 5G-мережах.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА КАТЕГОРІЇ ЗАСТОСУНКІВ

1.1 Периферійні обчислення з мультидоступом в мережах 5G. Стан та перспективи досліджень

Закон Мура передбачає, що швидкість процесора з часом експоненціально зростає [1]. Тому, кількість пристроїв Інтернету речей (IoT), які використовуються в галузях, що обслуговують застосунки на основі великих за обсягом наборів даних, невпинно зростає та потребує розширення можливостей обробки даних засобами мініатюрних пристроїв.

Зростає грамотність використання розумних пристроїв обширними групами громадян. Це дає змогу платформам на основі соціального Інтернету запускати громіздкі програмні засоби, що споживають пропускну здатність, щоб підвищити кількість підписок підвищеним рівнем якості обслуговування (QoS). За оцінками Cisco, кількість мобільних терміналів досягла трьох мільярдів 2020 року, а місячний трафік мобільних даних перевищив п’ятдесят екзабайт в 2021 році [2]. Таким чином, розгортання мільярдів «розумних» пристроїв вимагає від інтерфейсів доступу базових станцій мобільного зв’язку підвищення пропускної здатності.

Мобільна технологія п’ятого покоління (5G) – це фундаментальний прогрес, досліджений операторами мобільних мереж (MNO), щоб розширити обмеження існуючої архітектури мережі. Нові вимоги мобільних та обчислювальних мереж [3] сформовано щодо підвищеної:

– продуктивності;
– портативності;
– сумісності;
– еластичності;
– надійності;

– спектральної ефективності;

– енергоефективності.

Для досягнення зазначених вимог інноваційні мобільні мережі повинні дотримуватися відповідних підходів до програмного забезпечення мережі [4]. Зокрема основними етапами прокладання шляху до 5G та за межами мобільних парадигм 5G [5] є:

– віртуалізація;

– міграція сервісів;

– оркестровка;

– автоматизація сервісів у ланцюжках функцій служби [6].

Оскільки основні та транспортні частини нових мобільних мереж програмовані, то відомими методами для покращення мережі бездротового доступу [2] є:

– методи надзвичайно щільних мереж;

– множинні вводи та виходи (MIMO);

– високочастотний зв’язок.

Завдяки цим технологічним удосконаленням 5G гарантує збільшення пропускної здатності більш ніж у тисячу разів у порівнянні з попередніми поколіннями мереж.

Навіть із запрограмованою базовою мережею 5G задоволення різноманітних вимог, які вимагають пристрої на базі IoT, все ще є складним через недоліки існуючої інфраструктури надання послуг [7]. Звичайна архітектура хмарних обчислень не надає обширного переліку нових послуг [8]. Крім того, хмарні сервери фізично не здатні повсюдно обслуговувати мільярди IoT-пристроїв [9]. Ці обмеження в парадигмі хмарних обчислень посилюють уразливості, які можуть бути використані зловмисниками [10]. Конфіденційність є основною проблемою в моделях послуг на основі хмарних обчислень та аутсорсингу [11]. Більшість постачальників хмарних послуг порушують вимоги щодо конфіденційності місцезнаходження та даних споживачів.

Щоб подолати обмеження моделей послуг зберігання та опрацювання даних, в дев'яностих роках минулого століття була представлена парадигма «Edge Computing» (EC) з мережами доставки контенту (CDN), які децентралізували функції обробки даних [12]. Основна мета EC – розширення функцій від центрів хмарних обчислень до меж мобільної мережі [13]. Завдяки безпосередньому передаванню функцій до меж можна пом'якшити недоліки хмарної парадигми. Ця зміна архітектурної парадигми є причиною виникнення концепцій на основі 5G та за її межами для досягнення ґарантованих показників продуктивності. Існують різні варіанти концептів крайових обчислень для розширення цього поняття [2]:

– Периферійні обчислення з мультидоступом (MEC).

– Туманні обчислення Fog computing.

– Мобільні хмарні обчислення (MCC).

–Хмарні та Прозорі обчислення (TC).

5G та периферійні обчислення з мультидоступом можуть працювати незалежно. Але їх інтеграція дозволяє практично реалізувати застосунки та варіанти використання з підвищеними вимогами до наднадійності зв'язку з низькою затримкою та покращеними характеристиками безпеки та конфіденційності [14].

1.1.1 Безпекові загрози та ризики інноваційних мереж 5G

Основні перспективні вимоги до мереж 5G [15]:

– швидкість передачі даних – від одного до десяти Гбіт/с;

– затримка при передаванні даних в обидва боки – до одної мс;

– збільшена ємність для підключення пристроїв через канали з високою пропускною здатністю;

– очікувана доступність – 99,999%;

– стовідсоткове повсюдне підключення;

– покращення терміну служби батареї за рахунок зменшення витрат енергії на 90%.

Програмне забезпечення ядра 5G дає змогу сегментувати функції на багатошарову архітектуру з її особливою гнучкістю. Проект державно-приватного партнерства п’ятого покоління (5G-PPP) пропонує п’ять рівнів інфраструктури, мережі/контролю, оркестрації, бізнесу та послуг для формування функціональної архітектури 5G [16]:

1. Рівень оркестровки – дисперсна функція серед інших рівнів

2. Рівень інфраструктури – частина RAN-підключення мобільної мережі.

3. Рівень інфраструктури 5G – містить технології радіодоступу (RAT), що підтримують неортогональний множинний доступ (NOMA).

4. Рівень керування – реалізовує функції керування мережею.

5. Бізнес-рівень – мережа та бізнес-послуги.

При цьому рівень послуг – може бути представлений як розширення бізнес-рівня [4].

Заходи безпеки, спрямовані на забезпечення конфіденційності, цілісності, доступності, підзвітності, аутентифікації та авторизації, були впроваджені в попередніх мобільних мережах від 2G до довгострокової еволюції (LTE). Політика забезпечення інформації (IA) стала найглибшою для мереж 5G, оскільки необхідно забезпечити обробку, використання та передачу вмісту у кіберпросторі [17]. Шифрування є ключовим механізмом безпеки в мобільних мережах. Для цього використовуються схеми шифрування A3, A5/2, A5/3, A8, Kasumi, SNOW-3G і алгоритм шифрування (EEA) розвиненої пакетної системи (EPS) разом з алгоритмом цілісності EPS (EIA) [4].

Специфікації TS 23.122 і TS 33.210 визначають функції безпеки рівня доступу (AS) та бездоступного рівня (NAS) мобільних розгортань на основі проекту партнерства третього покоління (3GPP) [18]. AS і NAS є функціональними рівнями універсальної мобільної телекомунікаційної системи (UMTS) і стека протоколів LTE. Інноваційна інформаційно-технологічна архітектура 5G не дозволяє використовувати заходи безпеки старіших

поколінь мобільних мереж [19]. Крім того, автори [20] сформували перелік нових проблеми для мобільних мереж 5G:

– попит на мережевий трафік;
– безпека радіоінтерфейсу;
– цілісність користувацької площини;
– роумінг;
– атаки відмови в обслуговуванні (DoS)
– атаки насичення;
– сигнальні шторми.

Неоднорідна природа пристроїв із підтримкою 5G і технологіями IoT передбачає масову масштабованість із виникненням міжплатформних проблемам. Впровадження нових сервісів та застосунків неминуче призведе до залучення обширного кола користувачів та передплатників; отже, створення ситуації миттєвого попиту натовпу. Такі ситуації можуть використовуватися зловмисниками для перевантаження програмних та радіо інтерфейсів [21].

1.1.2 Безпекові загрози та ризики периферійних обчисленнь з мультидоступом

На відміну від інших парадигм крайових обчислень, периферійні обчислення з мультидоступом пропонується розгортати на контролері радіомережі (RNC), базовій станції (BS) або gNodeB (gNB) у термінах 5G [13]. Тому вони більше залежать від якості обслуговування. Архітектура периферійних обчисленнь з мультидоступом, визначена ETSI, складається з рівня краю/хоста та системного рівня [22]. Ці два рівні сегментують функції реєстрації послуг та надання послуг для покращення доступу та безпеки. Однак нові структури та технології віртуалізації для розгортання динамічного середовища обслуговування, формують безпрецедентні проблеми безпеки та конфіденційності. Операційна структура периферійних обчисленнь з мультидоступом, подана на рисунку 1.1 визначена ETSI [23].

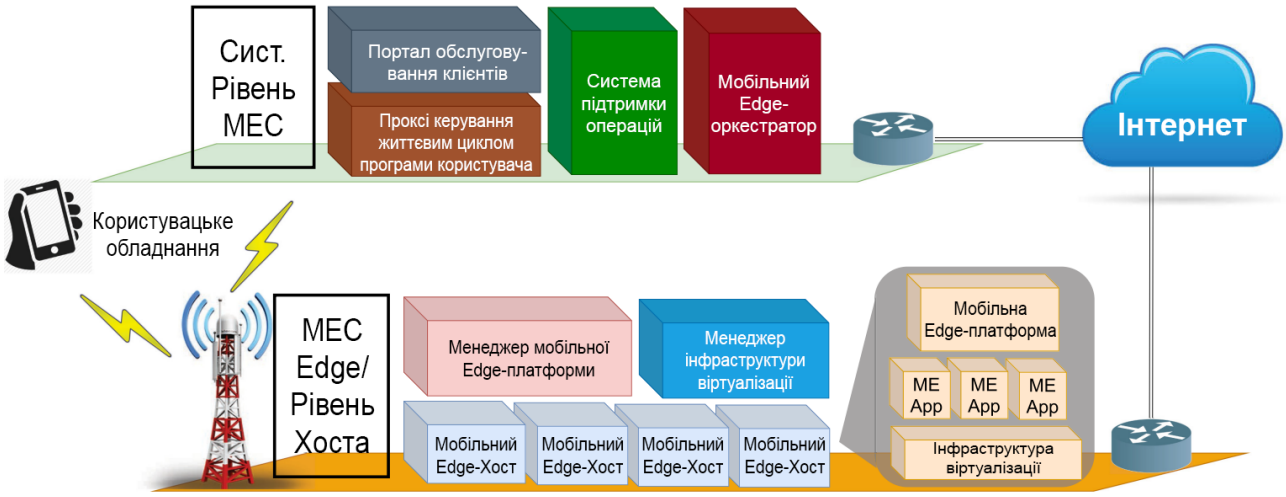

Рисунок 1.1 – Структура та функціонування MEC

Функції схвалення, відхилення та керування запитами на обслуговування обробляються сутностями проксі-сервера керування життєвим циклом застосунків користувача, порталом обслуговування клієнта та системою підтримки операцій. Мобільний Edge оркестратор оркеструє всю систему в своєму домені. Мобільні граничні хости (МЕН) – це налаштовані відповідно до вимог абонентського обслуговування віртуальні об’єкти. Виявлення вразливостей і загроз у розгортанні периферійних обчисленнь з мультидоступом на базі 5G слід розглядати в кожному конкретному випадку використання.

1.2 Категорії застосунків що використовують периферійні обчислення з мультидоступом в мережах 5G

Розглянемо перспективні випадки використання периферійних обчислень з мультидоступом. Варіанти використання подані на рисунку 1.2 розглядаються як послуги для споживачів 5G [23]:

– Критична інфраструктура.
– Покращені мобільні та медійні широкосмугові канали.
– Міжмашина взаємодія (M2M) для IoT.
– Взаємодія між транспортними засобами (V2V).

– Доповнена, віртуальна та змішана реальність (MR).
– Безпілотні літальні апарати (БПЛА).

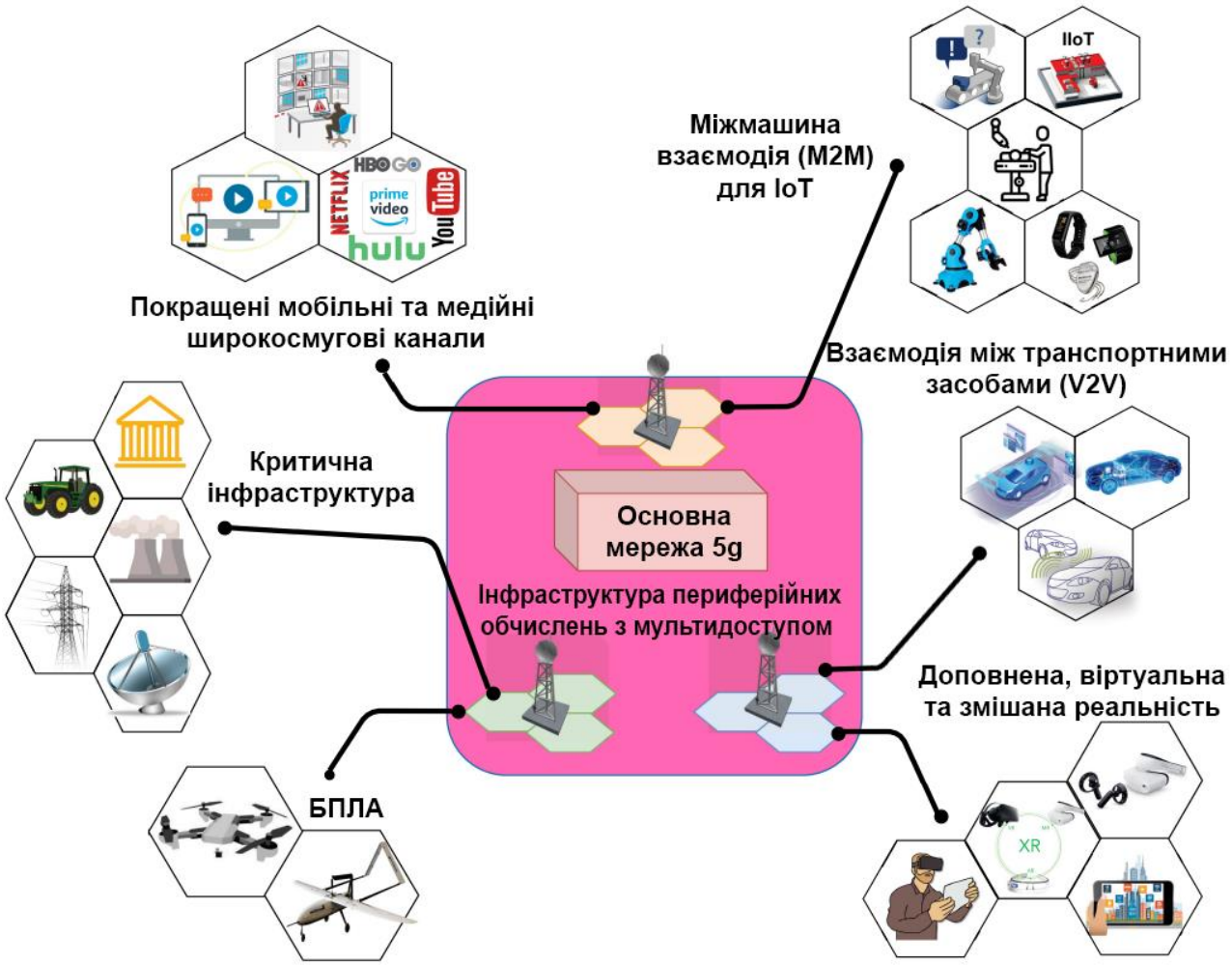

Рисунок 1.2 – Варіанти використання 5G та периферійних обчислень з мультидоступом

При цьому якість обслуговування QoS та якість досвіду (QoE) є ключовими факторами та безпосередньо формують фартість конкретної послуги [24].

1.2.1 Критична інфраструктура

Впродовж останнього періоду часу завдяки оцифруванню систем управління на основі інформаційної технології IoT суттєво розширилась сфера

застосунків для послуг на основі критичної інфраструктури [25]:

– енергетика;

– водопостачання;

– каналізація;

– морські бурові установки;

– фінансові застосунки;

– аварійні служби.

Глобальне розширення зазначених послуг та розосередження глобальних кластерів обмежує можливості використання централізованих засобів обробки даних. Координована група «Європейського комітету стандартизації» – «Європейського комітету з електротехнічної стандартизації» – «Європейського інституту телекомунікаційних стандартів» («CEN-CENELEC-ETSI») запропонувала інформаційно-технологічну архітектурну модель «Розумних GRID» подану на рисунку 1.3 [23].

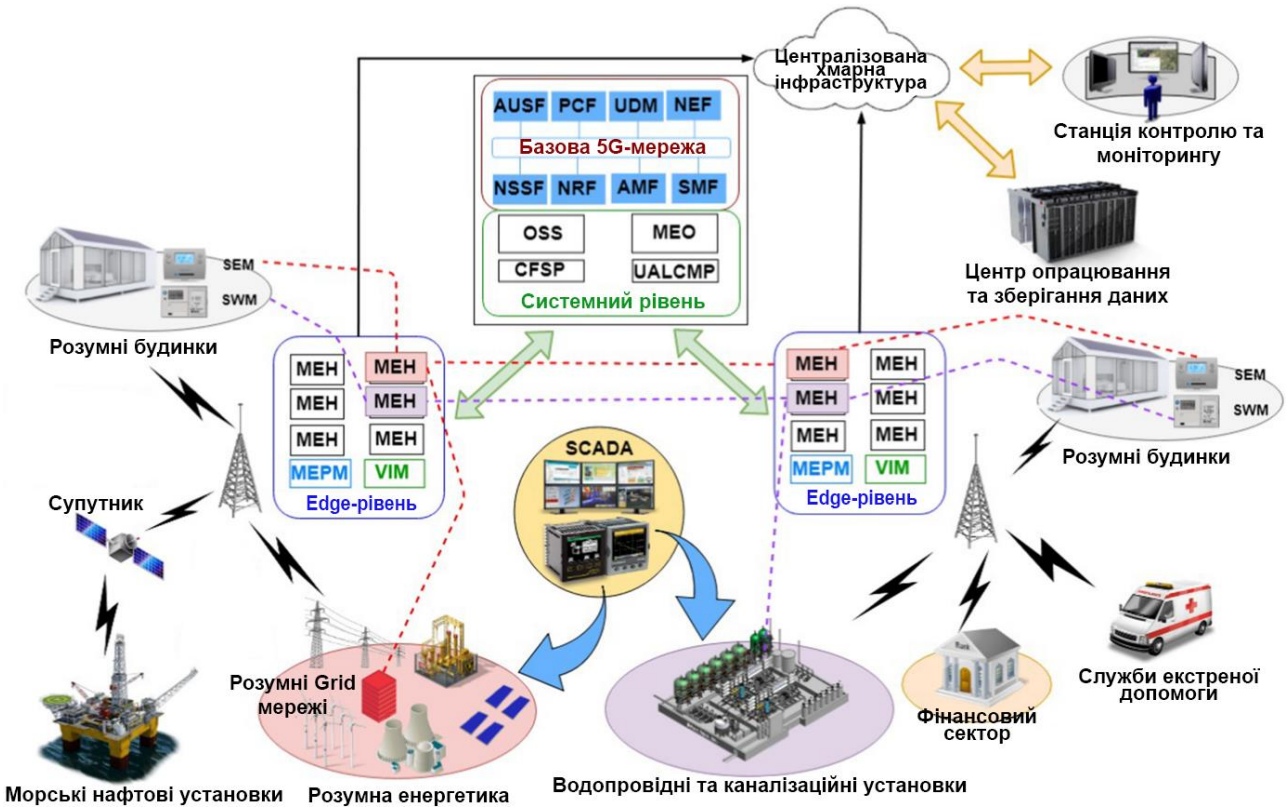

Рисунок 1.3 – Підключення критичної інфраструктури до платформи MEC

При цьому виокремлено три виміри та п’ять рівнів функціональної сумісності з доменами та зонами енергетичного сектору, який керує енергосистемою. Децентралізований характер «розумних» мереж в енергетичних системах та вимога мінімізації затримок передачі критичних параметрів [26] потребують розгортання периферійних обчислень з мультидоступом.

Інтеграція інформаційно-технологічних платформ периферійних обчислень з мультидоступом для послуг критичної інфраструктури є високоімовірною та покращить взаємодію широких громадських груп користувачів з послугами [27].

1.2.2 Покращені мобільні та медійні широкосмугові канали

На рисунку 1.4 зображено послуги на основі AR та потокового відео, які можна розгортати в інфраструктурі послуг периферійних обчислень з мультидоступом [23].

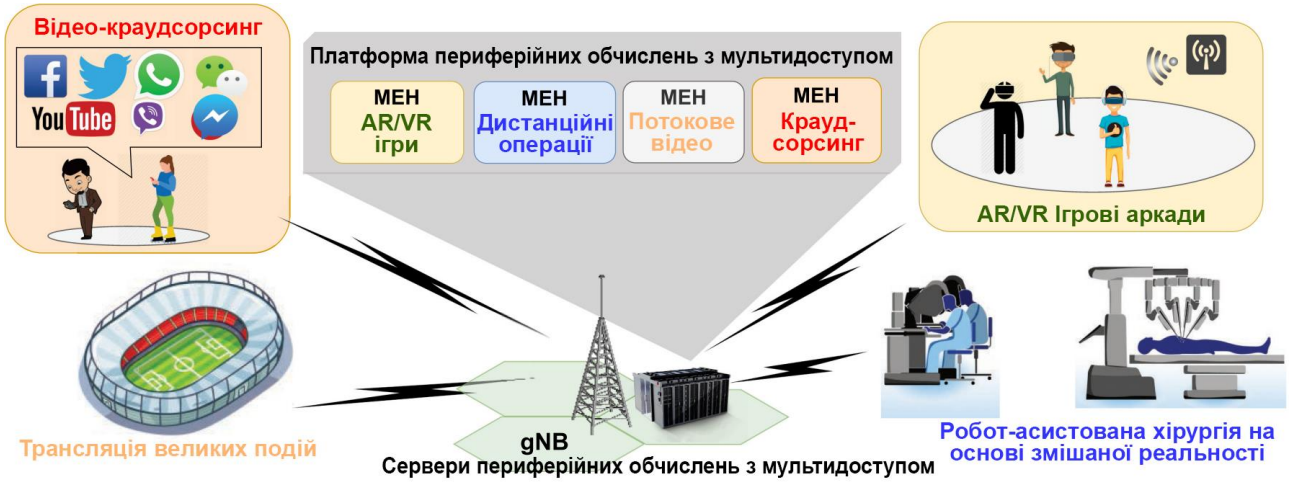

Рисунок 1.4 – Інноваційні послуги на основі AR та потокового відео

Категорія застосунків покращених мобільних та медійних широкосмугових каналів містить:

– покращені мобільні широкосмугові канали;

– потокове відео;
– потокова аналітика;
– великі за розмірами інформаційно-технологічні події.

На даний час активно використовуються застосунки на основі аналізу відеопотоку для розпізнавання автомобільних номерних знаків та облич, домашнього та громадського спостереження. Вони вимагають високої обчислювальної складності алгоритмів та, як наслідок, залежать від UHD-передачі [28]. Краудсорсингові медіа-дані швидко завантажуються на сервери через зростаючі мультимедійні канали YouTube, Facebook, WhatsApp та Instagram [29]. Тому зростає необхідність впровадження заходів щодо оптимізації пропускної спроможності мережевих потокових сервісів.

1.2.3 Міжмашина взаємодія (M2M) для IoT

У цій категорії доцільно розглянути застосунки для носимих пристроїв електронного здоров’я, IoT-пристрої та весь спектр керованих машинами автоматизованих комунікацій [27]. Рівень сприйняття переважної більшості IoT-застосунків сформовано з сенсорних пристроїв та виконавчих механізмів, які використовують M2M-зв’язок для передачі даних та керуючих сигналів. Для M2M-взаємодії здебільшого використовуються нестільникові інформаційні технології [30], зокрема:

– ультраширокосмуговий зв’язок (UWB);
– WLAN;
– ZigBee;
– Bluetooth;
– LPWA;
– LoRa;
– вузькосмуговий IoT (NB-IoT);
– Wireless Body Area Networks (WBAN) в галузі електронного здоров’я.

Реалізація послуг на основі IoT охоплює діапазон типів зв'язку, який варіюється від людини до людини (H2H), від людини до машини (H2M) або навпаки, і від машини до машини (M2M) [31]. На рисунку 1.5 подано застосунки з використанням периферійних обчислень з мультидоступом.

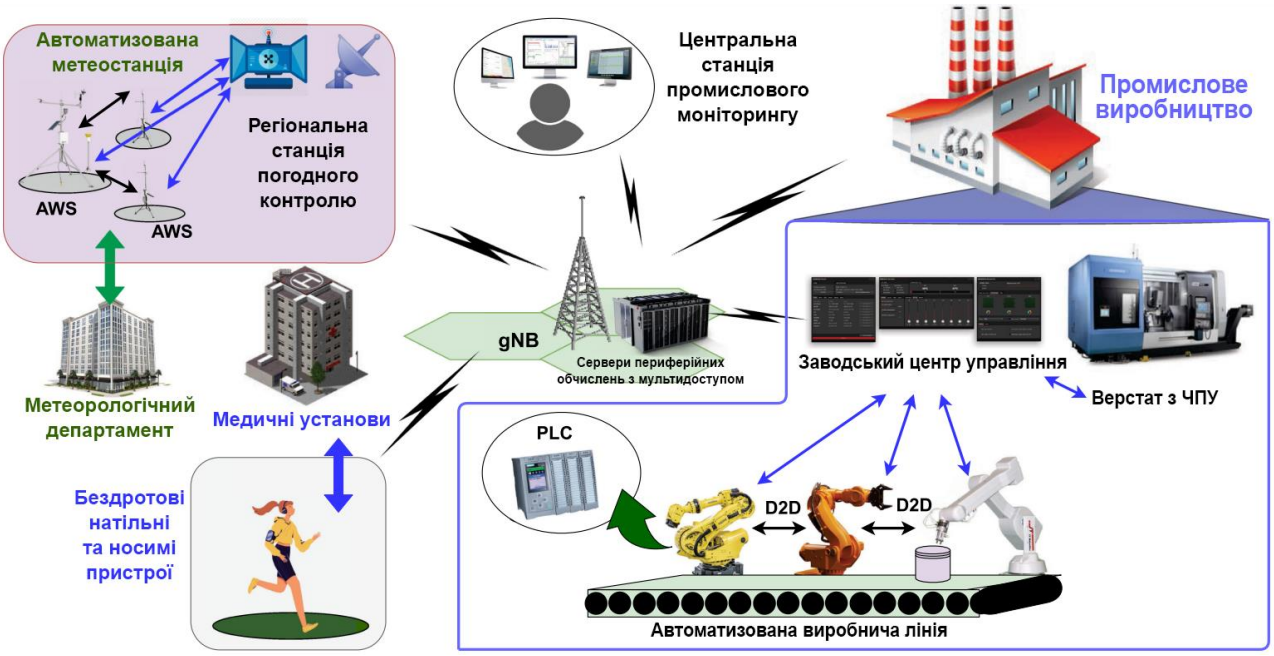

Рисунок 1.5 – Інтеграція міжмашинної взаємодії та периферійних обчислень з мультидоступом

В галузі охорони здоров'я застосовуються роботи для допомоги здоров'ю, проведення віддалених операції та дистанційного моніторингу пацієнтів [13]. Зокрема імплантовані серцеві дефібрилятори, кардіостимулятори, нейростимулятори, глюкометри, оксиметри та монітори життєво важливих показників [32].

1.2.4 Взаємодія між транспортними засобами

Категорія взаємодії між транспортними засобами включає:

– Канали автономного водіння.

– Підключені транспортні засоби.

– Взаємодію між транспортними засобами (V2V) тощо.

Адаптація V2E є ініціативою для інтелектуальних транспортних систем (ITS) [33]. Транспортні мережі (VN) формують розгортання ITC та посідають особливе місце в контексті 5G [34] (див. рисунок 1.6).

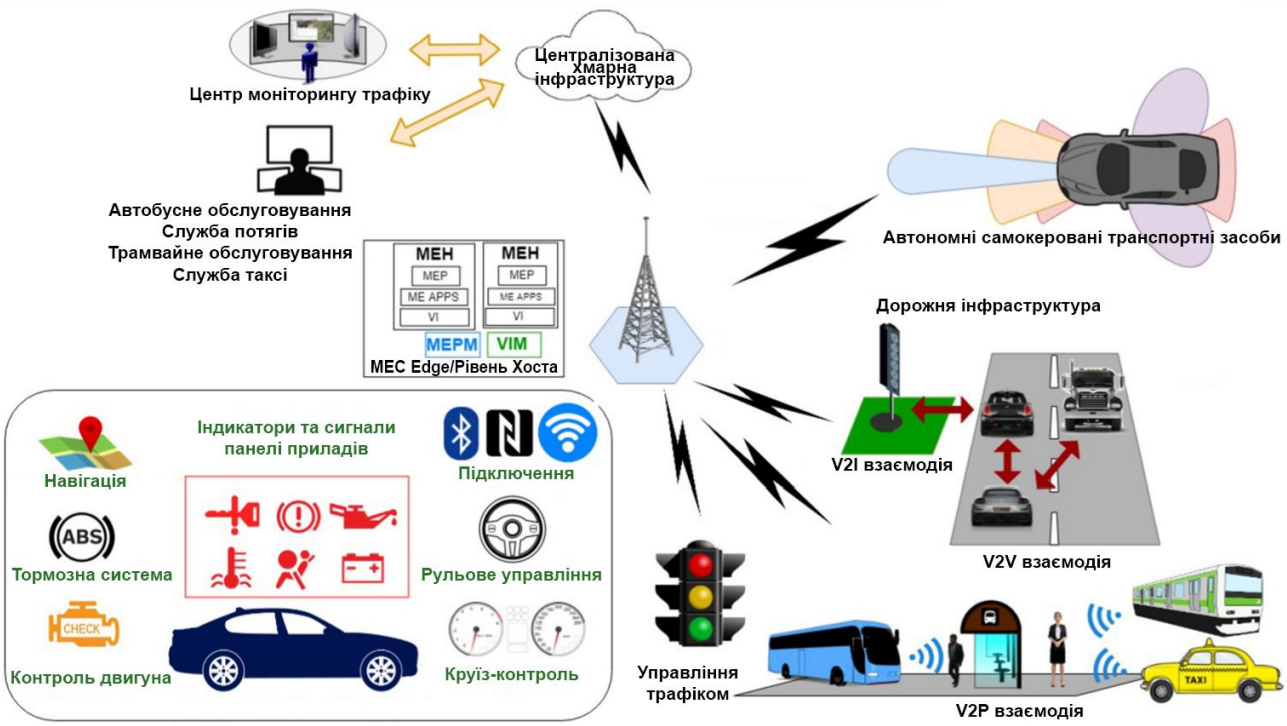

Рисунок 1.6 – Інтеграція V2V з та периферійних обчислень з мультидоступом

Використання системи периферійних обчислень з мультидоступом або будь-якої іншої периферійної парадигми обґрунтоване для запуску застосунків V2E через вимоги щодо наднизької затримки та високої надійності [13]. Внаслідок передбачуваного різкого розвитку транспортної галузі її інфраструктури стають вагомими цілями для кібер-злочинців через мобільну структуру [35].

1.2.5 Доповнена, віртуальна та змішана реальність

5G AR, VR та MR розширюють спенктр послуг [36] інтерактивного занурення та досвіду для:

– 5G-точок доступу;
– автомобільних систем;
– інформаційно-розважальних ігор;
– навчально інструктажних застосунків;
– застосунків інтелектуального здоров’я;
– застосунків дистанційної хірургії
– дистанційного роботизованого керування [37].

VR відноситься до цілком імітованої візуалізації. AR та MR відрізняються за ступенем віртуалізації, накладеної на візуальне сприйняття внаслідок оцифрування [38]. Типовий VR-дисплей «Head Mounted Display» (HMD) закриває поле зору користувачів та розташовує віртуалізовані елементи за допомогою відстеження руху очей та голови. На сучасному ринку послуги віртуальної реальності делегуються недорогим мобільним пристроям «Samsung Gear VR» та «Google Cardboard». Водночас «Oculus Rift», «HTC Vive» або «PlayStation VR» є високоякісними потоковими інформаційно-технологічними продуктами, чутливими до затримок передавання даних. Для інтеграції периферійних обчислень з мультидоступом [28] та AR-застосунків використовуються мобільні технології Google goggles, Layar, Wikitude та Junaio.

Типовий AR-процес вимагає роботи п’яти важливих компонентів: джерело відео, трекер, картограф, розпізнавання об’єкта та засіб візуалізації. Всі перелічені компоненти крім джерела відео та рендерера можуть інтегруватись з локальними серверами периферійних обчислень з мультидоступом для інтенсивного розвантаження централізованих систем [39].

1.2.6 БПЛА

Зростає роль БПЛА в різних сценаріях, зокрема – реагування на надзвичайні ситуації та стихійні лиха, фотографування та інспектування, точне землеробство та екологічний моніторинг, військова галузь, ретрансляція зв’язку та контроль руху, надання допомоги та оперативна доставка вантажів [40].

БПЛА класифікуються на маловисотні (LAP) та висотні платформи (HAP) [41]. Вони розрізняються за висотою, обчислювальними здатностями, покриттям, потужністю, місткістю та витривалістю.

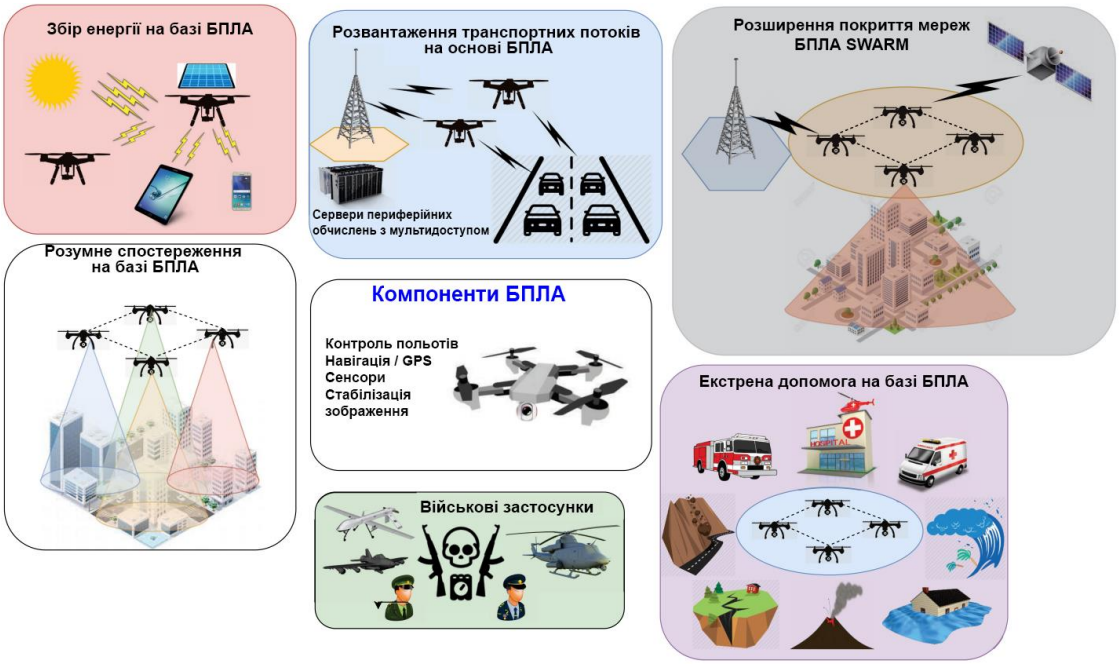

Рисунок 1.7 – Застосунки БПЛА на базі периферійних обчислень з мультидоступом

Використання надійних криптографічних примітивів або тривалих протоколів безпеки є неможливим, оскільки, розмір, вага та потужність БПЛА є обмеженнями для досягнення бажаних показників продуктивності. Пріоритетним завданням БПЛА є збереження терміну служби акумулятора для польотів, одночасно вивантажуючи обчислювальний вміст або вміст зберігання на сервери периферійні обчислення з мультидоступом для обробки [13].

1.3 Висновок до першого розділу

В першому розділі кваліфікаційної роботи проаналізовано стан та перспективи досліджень в галузі периферійних обчислень з мультидоступом в мережах 5G та описано категорії застосунків що їх використовують.

РОЗДІЛ 2. АНАЛІЗ БЕЗПЕКИ ПЕРИФЕРІЙНИХ ОБЧИСЛЕНЬ З МУЛЬТИДОСТУПОМ В МЕРЕЖАХ 5G

2.1 Уразливості безпеки та існуючі рішення для захисту периферійних обчислень з мультидоступом в мережах 5G

2.1.1 Критична інфраструктура

На основі припущення, щодо внутрішні зв’язки об’єктів критичної інфраструктури захищені проєктом, можна зробити висновок, що двонаправлений зв’язок з базовими станціями може бути єдиним вектором, який слід розглядати для втручання зловмисників. Загрози такому підключенню будуть подібні до будь-яких атаки, базованих на вторгненнях, втручаннях, DoS або розподілених DoS-атаках (DDoS). Вони можуть припинити доступ до запущених на периферії відповідних інфраструктурних служб застосунків. Чез збільшення масштабів застосунків, об’єкти граничного рівня периферійних обчислень з мультидоступом повинні передплатити більше одного МЕН. При цьому георозподілений характер понинен пов’язувати більше ніж один граничний рівень МЕС або рівні системи для певної послуги на основі критичної інфраструктури. Це збільшує можливість атаки або зараження зловмисним агентом через сервер МЕС.

Розпорошене розгортання SEM у домогосподарствах в інсталяції інтелектуальної мережі на основі AMI спонукає зловмисників здійснювати атаки [42]:

– підслуховування;
– модифікації;
– переривання в каналах бездротового зв’язку;
– фізичного пошкодження в безпосередній близькості.

Також в середовищах інтелектуальних мереж високоймовірними є атаки позбавлення сну (SDT) та атаки виснаження батареї (BEA) [43]. Зазначені

зловмисні впливи спрямовані на установки SWM та в сценаріях «розумного» управління ресурсами. Однак характер атак залежить від сценаріїв розгортання застосунків та програмно-алгоритмічних засобів критичної інфраструктури.

Оскільки основні функції застосунків для обслуговування критичної інфраструктури реалізуються засобами SCADA-систем, вразливості внутрішньої безпеки є загальними для всіх випадків практичної реалізації. Ізольований і відокремлений характер SCADA-систем раніше забезпечував високу стійкість до кібератак [44]. Однак у системах SCADA були виявлені загрози та вразливості, наприклад у випадку з популярним хробаком STUXNET, що підвищило ймовірність уразливості критичних інфраструктурних служб [45]. Приклад скомпрометованих SCADA-систем [46]:

– втручання в каналізаційну систему в м. Маручі в Австралії;
– троян «BlackEnergy», спрямований на українську енергосистему;
– зловмисне програмне забезпечення HAVEX;
– атака з ін’єкцією команд на водоочисну станцію в Кемурі.

Зв'язок установок SCADA здійснюється за допомогою протоколів Modbus, DNP3 і Profibus [47]. Кібератаки, ймовірні на програмовані логічні контролери (ПЛК), поділяються на [46]:

– розвідувальні;
– командні;
– ін’єкції відповіді;
– DoS-атаки.

При цьому система МЕС буде проникнути з боку критичної інфраструктури. Наприклад, розподілена природа розумних мереж дозволить скомпроментованій «розумній» мережі розбалансувати енергетичне навантаження, передаючи оманливу інформацію периферійним об’єктам. Це може призвести до катастрофічних обставин.

Зв’язок вузлів критичної інфраструктури з найближчою базовою станцією має бути забезпечено ефективними криптографічними засобами через їхню критичність та властиві ресурси. Пріоритетом для протоколів зв'язку буде

безпека, незважаючи на затримки та використання пропускної здатності. Хоча заходи безпеки, які вживаються внутрішньо, відрізняються для різних практичних реалізацій. Безпекові загрози під час оновлення центральних станцій моніторингу [23] показано на рисунку 2.1.

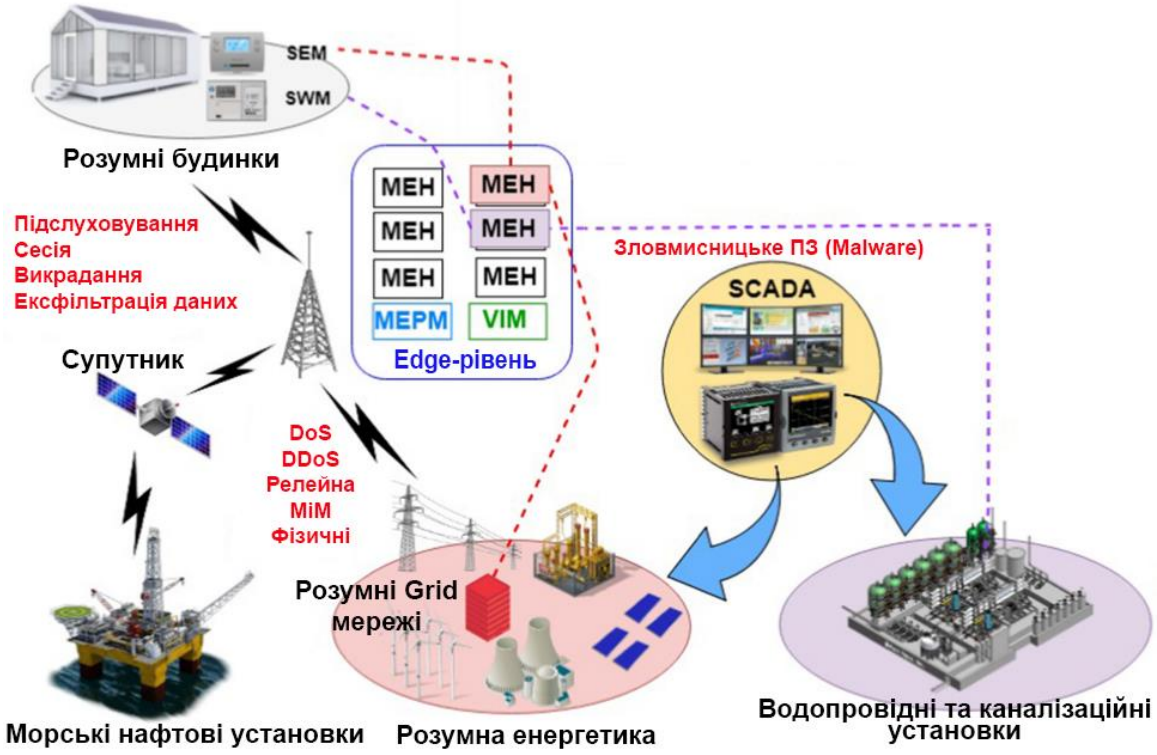

Рисунок 2.1 – Безпекові загрози при підключенні критичної інфраструктури до платформи периферійних обчислень з мультидоступом в мережах 5G

Оскільки шкідливі програми є вагомою загрозою для SCADA-систем, то Ширазі [47] запропонований підхід для виявлення аномалій у SCADA-системах. Підхід сформовано з використанням методів машинного навчання. Зокрема використано методи «K-середнє» та «наївні байєсівські значення» в контрольованому режимі. Аналіз основних компонентів проведено з використанням методів «розкладання сингулярних значень» (PCA-SVD) та «моделі гаусової суміші» (GMM) в неконтрольованому режимі.

Хуссейн [48] опублікував модель розподілу ресурсів на основі периферійних обчислень для використання в існуючих системах хмарних

центрів обробки даних, схильних до затримок при обміні даними через супутники.

Лелігу [49] запропонував чотирирівневу структуру, яка містить:

– енергетичний рівень;
– телекомунікаційний рівень;
– VNF-рівень;
– прикладний рівень.

Фреймворк використовує периферійні обчислення з мультидоступом як розширення технології мультирадіодоступу (RAT) для забезпечення розвантаження з VNF-дескрипторами на основі блокчейну. Зазначены VNFD-декриптори використовуються як теги процесу для досягнення відстежуваності в енергетичному шарі. Однак в роботі [49] недостатньо розкрито сценарій розгортання для розвантаження xMEC.

2.1.2 Покращені мобільні та медійні широкосмугові канали

Високоймовірно, що перехоплення відеопотоку можливий за розкрадання зловмисниками для вилучення підроблених облікових даних, які порушують цілісність вмісту [50]. Маніпуляції зі стрічкою новин призводять до оманливих обставин для глядачів і будуть критичними залежно від ентропії інформації. Оскільки більшість потокового відеотрафіку генерується з краудсорсингових програм, заражене периферійне обладнання створює загрозу багаторазового передачі шкідливого вмісту, який використовується як точка виходу через канали потокового відео. Більшість облікових записів у соціальних мережах і краудсорсингу не мають надійних облікових даних на основі пароля. Тому фішингові атаки здатні захопити такі облікові записи та порушують цілісність. Цей тип атаки призводить до компрометації периферійної інфраструктури. Однак канали потокового відео кодуються з прийнятним рівнем шифрування. Це робить проміжні атаки менш імовірними.

Макінен [51] запропонував бізнес-модель для потокового відео в обробці подій, що включає платформи обслуговування периферійних обчислень з мультидоступом в мережах 5G. Для бізнес-моделі проаналізовано критерії сервісу та технологій, організації та фінансового дизайну. Білал [29] опублікували відомості щодо інформаційно-технологічних рішень на основі периферійних обчислень для інтерактивних потокових та ігрових спільнот.

2.1.3 Міжмашина взаємодія (M2M) для IoT

Ця категорія застосунків успадковує три основні вразливості:

– засоби зв'язку, зокрема прослуховування радіоканалу;
– дефіцит енергетичних ресурсів;
– обмеженість обчислювальних ресурсів.

Водночас на нано-вузли в WBAN поширені атаки [32]:

– DoS;
– заглушення;
– підробка даних.

Запропонована в [52] «розумна структура», полегшує процес вилучення, перетворення та завантаження даних для стратегії пошуку вразливих даних. Лі [53] запропонував нову структуру, яка інтегрує M2M-зв'язок з периферійними обчисленнями з мультидоступом у віртуалізовану стільникову мережу для розвантаження обчислювальних завдань та вдосконалення процесів енергоспоживання. Чжан [54] запропонував схему підвищення QoS з обмеженою затримкою для двох типів сценаріїв розвантаження мобільних даних. В свою чергу Донг [55] запропонував підхід ICN для підтримки anycast-послуг в базовій мережі через залучення в граничній мобільній мережі. Результати показують, що економія пропускної спроможності вища при менших інтервалах anycast-оновлення. Бракен [56] пропонує архітектуру «Edge Supportive Secure MAR» в медичній галузі.

2.1.4 Взаємодія між транспортними засобами

Автотранспортні інформаційно-технологічні системи та структури схильні до запущених поблизу цільового пристрою атак, зокрема, фізичних пошкоджень, апаратних троянських програм та атаки з супутніх інформаційних каналів. Ці атаки можуть надати доступ до комунікаційних пристроїв «розумних» транспортних засобів, які безпосередньо підключені до блоку керування двигуном (ECU) автомобіля. Проникнення в ECU може призвести до обходу критичних систем безпеки транспортного засобу [33]. Вплив на електронний блок управління в процесі автономного або напівавтономного керування може загрожувати транспортному засобу та пасажирам. Заражена та дискредитована інформаційна система може передати неправдиву інформацію до застосунків та систем вищого рівня щоб спричинити дорожньо-транспортні пригоди з порушенням роботи процесів пересування обширного переліку автомобілів. Імоваірні для транспортних засобів загрози здебільшого націлені на різні підсистеми окремого транспортного засобу [33], зокрема:

– підробка та перешкоджання GPS;
– атака на внутрішні пристрої;
– зловмисне програмне забезпечення;
– атака на головний блок;
– атака на акустичні давачі з підробленням шумів або перешкод;
– заглушення радарів, повторювачі, шуми та «розумні» матеріали;
– заглушення LIDAR або «розумні матеріали»
– атака на магнітний або тепловий одометричний датчик;
– атаки – електромагнітні імпульси на електронні пристрої.

В окрему категорію можна виділити атаки на мережу контролерів (CAN) [57], зокрема:

– словник;
– райдужна таблиця;
– атаки грубої сили для вилучення паролів або ключів;

– DoS або DDoS атаки для порушення роботи служб;

– атаки на основі протоколу, спрямовані на, або оновлення FlexRay та Rouge;

– прошивка ECU є вірогідною атакою з точки зору програмного забезпечення.

Традиційні заходи захисту автомобільних систем є нежиттєздатними через пришвидшений розвиток інфраструктури програмного забезпечення концепції підключеного транспортного засобу.

Мобільність під’єднаних транспортних засобів буде серйозною проблемою, оскільки їх швидкість і напрям швидко змінюються з рухом. Цей аспект мобільності додатків V2E схильний до загроз перехоплення частоти переміщеного каналу, маскування під час взаємодії та атак міграції [58]. Ця категорія кібер-загроз може призвести до заторів на дорогах, аварій, пошкодження майна або людських жертв.

Щоб протистояти загрозам безпеки під час розгортання інформаційних та комунікаційних технологій, в стандарті «IEEE Wireless Access for Vehicular Environments» (WAVE) були визначені процедури та алгоритми безпеки в США та Європі відповідно до ETSI [59]. Ґрів [60] обговорював периферійні обчислення з мультидоступом для зменшення пов'язаних з алгоритмами з великими ресурсами обчислювальних витрат і затримок в хмарі для систем «ADAS Electronic Horizon».

2.1.5 Доповнена, віртуальна та змішана реальність

Основні загрози в AR-застосунках – це доступ до відеопотоків і несанкціоновані маніпуляції з ними, коли зловмисник може легко перебрати конфіденційні дані користувачів [50]. Маніпуляції з відеопотоками можуть призвести до критичних збоїв у машинах у промислових застсоунках [39] . Експлуатований потоковий канал між серверами периферійних обчислень з мультидоступом в мережах 5G та AR-застосунками може конфіскувати вміст на

хостах та заражати потоковий трафік. Заражений МЕ-застосунок маніпулюватиме даними обчислювальних серверів, щоб виділити більше несуттєвих ресурсів для конкретної програми та спричинити переривання обслуговування хостів [61].

Ланґфінджер [50] запропонував безпечну архітектуру для промислових AR-застосунків, сумісну з стандартизацією Індустрії 4.0. Цяо. запропонував структуру [62] для інтеграції веб-AR та периферійних обчислень з мультидоступом в мережах 5G. Елбамбі [38] досліджував варіанти використання багатокористувацьких сценаріїв інтерактивних ігор у віртуальній реальності для оцінки продуктивності використання граничних обчислень.

2.1.6 БПЛА

У цій категорії використання криптографічних примітивів обмежено через вимогу збереження обчислювальної потужності, наприклад, для дронів. Вірогідні для БПЛА загрози класифікуються за [63]:

– електронними та електромагнітними;
– кібернетичними
– фізичними просторами (ECP).

Найпоширенішим типом атаки для дронів або БПЛА є GPS-спуфінг. При цьому фальшиві GPS-координати місцезнаходження надсилаються до БПЛА для введення в оману або збою об’єкта. В [63] розглянуто компрометуючі випромінювання для обходу криптографічних заходів з електромагнітними, оптичними або акустичними випромінюваннями. Крім того, є високоймовірними є спрямовані на виснаження батареї БПЛА [64] атаки:

– шкідливе програмне забезпечення;
– логгери;
– засліплення віддаленого пілота за допомогою лазера;
– підробка ідентифікаційних даних;
– багатошаровість;

– багатопротокольність;

– різні DoS або DDoS-атаки.

Фоуда [63] провела комплексну оцінку ймовірних атак на системи БПЛА, зосереджуючись на архітектурі UAS на основі програмно-визначеного радіо (SDR). Хупер [65] запропонував багаторівневу структуру безпеки, яка інтегрує рівні моделі OSI з ядром операційної системи Linux, щоб захистити БПЛА типу «Parrot Bebop» від переповнення буфера експлойтів, DoS і кешу протоколу розділення адрес (ARP) тощо.

2.2 Результати аналізу вразливостей безпеки

На основі проведеного аналізу наукових літературних джерел сформуємо опис пов’язаних з використанням апаратних платформ периферійних обчислень з мультидоступом в мережах 5G [23] безпекових проблем та подамо його в таблиці 2.1.

Таблиця 2.1 – Опис безпекових проблем пов’язаних з використанням апаратних платформ периферійних обчислень з мультидоступом та 5G

Безпекові загрози	**Опис**
1	**2**
DoS/DDoS та перешкоди	Зловмисні запити на обслуговування, націлені на радіоінтерфейси 5G та периферійні обчислення з мультидоступом (UALCMP і CFSP), створюються в цифровому середовищі та призводять до затримок і збоїв у роботі.
Недоліки PLC/SCADA/ CPS	Недоліки конструкції апаратних засобів викривають та дискредитують системи промислової автоматизації.

Продовження таблиці 2.1

1	2
Виснаження енергії та ресурсів	Кінцевою метою зловмисників націлених на вичерпування ресурсів обробки, зберігання та пам’яті є виснаження автономних джерел енергії IoT-пристроїв.

Продовжуючи аналіз наукових літературних джерел, сформуємо опис безпекових проблеми пов’язаних з масштабованістю програмно-алгоритмічних засобів периферійних обчислень з мультидоступом в мережах 5G [23] та подамо його в таблиці 2.2.

Таблиця 2.2 – Опис безпекових проблем пов’язаних з масштабованістю засобів периферійних обчислень з мультидоступом та 5G

Безпекові загрози	Опис
Фішинг, маскування, самопро-голошення та порушення доброчесності	Неможливість перевірити або підтвердити унікальний ідентифікатор точок доступу або інтерфейсів 5G та периферійних обчислення з мультидоступом дозволяє зловмисникам видавати себе офіційні служби та видобувати інформацію з підміненим рівнем доступу.
Масштабованість	Міріади пристроїв IoT вимагають швидкого доступу до послуг периферійних обчислень з мультидоступом, тому громіздкі криптопримітиви непридатні.
Сумісність	Технологічна диверсифікація, властива 5G та IoT, обмежує інтеграцію стандартизованих заходів безпеки.

Узагальнюючи аналіз наукових літературних джерел, сформуємо класифікацію безпекових проблем по категоріях використання периферійних обчислень з мультидоступом в мережах 5G [23] та подамо його в таблиці 2.3.

Таблиця 2.3 – Безпекові проблеми по категоріях використання периферійних обчислень з мультидоступом в мережах 5G

Категорія / **Безпекові загрози**	**Критична інфраструктура**	**Мобільні та медійні широкосмугові канали**	**Міжмашина взаємодія**	**Взаємодія між транспортними засобами**	**Доповнена, віртуальна та змішана реальність**	**БПЛА**
DoS/DDoS та перешкоди	В	С	В	С	С	В
Недоліки PLC/SCADA/ CPS	В	Н	В	С	Н	Н
Виснаження енергії та ресурсів	С	С	В	В	С	В
Фішинг, маскування, самопро-голошення та порушення доброчесності	Н	С	В	В	С	В
Масштабованість	С	С	В	Н	С	С
Сумісність	Н	В	В	С	С	С

В табл. 2.3 позначено:

– В – високий рівень загроз;

– С – середній рівень загроз;

– Н – низький рівень загроз.

2.3 Результати аналізу існуючих рішень щодо запобігання та протидії вразливостям безпеки

На основі проведеного аналізу наукових літературних джерел сформуємо перелік криптографічних та Блокчейн-методів та контрзаходів безпеки при використанні периферійних обчислень з мультидоступом в мережах 5G [23] та подамо його в таблиці 2.4.

Таблиця 2.4 – Криптографічні та Блокчейн-методи і контрзаходи безпеки при використанні периферійних обчислень з мультидоступом в мережах 5G

Категорія / **Контрзаходи та безпекові методи**	**Критична інфраструктура**	**Мобільні та медійні широкосмугові канали**	**Міжмашина взаємодія**	**Взаємодія між транспортними засобами**	**Доповнена, віртуальна та змішана реальність**	**БПЛА**	**Джерело**
Використання VNF-дескрипторів на основі блокчейну для відстеження рівня енергоефективності	Так	Ні	Так	Ні	Ні	Ні	[49]
Блокчей-модель для запобігання та протидії пов'язаних з енергоефективністю атак	Так	Так	Так	Ні	Ні	Ні	[43]
Криптографічні засоби в механізмі аутентифікації для балансування енергоефективності БПЛА	Ні	Ні	Ні	Так	Ні	Так	[35]

Продовжуючи аналіз наукових літературних джерел, сформуємо перелік методів виявлення аномалій та контрзаходів безпеки при використанні периферійних обчислень з мультидоступом в мережах 5G [23] і подамо його в таблиці 2.5.

Таблиця 2.5 – Методи виявлення аномалій та контрзаходи безпеки при використанні периферійних обчислень з мультидоступом в мережах 5G

Категорія / **Методи та контрзаходи**	**Критична інфраструктура**	**Мобільні та медійні широкосмугові канали**	**Міжмашина взаємодія**	**Взаємодія між транспортними засобами**	**Доповнена, віртуальна та змішана реальність**	**БПЛА**	**Джерело**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Методика виявлення аномалій на основі	Так	Ні	Так	Ні	Ні	Ні	[47]

Продовження таблиці 2.5

1	2	3	4	5	6	7	8
алгоритмів машинного навчання для SCADA-систем							
Заходи безпеки та конфіденційності в інтегрованому сценарії енергорозвантаження	Ні	Ні	Ні	Так	Ні	Так	[60]

Перелік інформаційно-технологічних архітектур та структур для підвищення рівня безпеки при використанні периферійних обчислень з мультидоступом в мережах 5G [23] і подамо його в таблиці 2.6.

Таблиця 2.6 – Безпекові інформаційно-технологічні архітектури та структури при використанні периферійних обчислень з мультидоступом в мережах 5G

Категорія **Безпекові інформаційно-технологічні архітектури та структури**	**Критична інфраструктура**	**Мобільні та медійні широкосмугові канали**	**Міжмашина взаємодія**	**Взаємодія між транспортними засобами**	**Доповнена, віртуальна та змішана реальність**	**БПЛА**	**Джерело**
Архітектура для промислових AR-застосунків для формування безпечних обчислювальних конвеєрів	Так	Так	Ні	Ні	Так	Ні	[50]
Легітимація об’єктів із серверів в інформаційно-технологічній архітектурі для процесу зарядки транспортних засобів	Так	Ні	Ні	Так	Ні	Ні	[66]
Багаторівнева структура безпеки для БПЛА з інтеграцією моделі OSI	Ні	Ні	Ні	Ні	Ні	Так	[65]
«Розумний фреймворк» для виявлення аномалій у видобутих даних	Так	Ні	Так	Ні	Ні	Ні	[52]
Безпека як послуга (SECaaS) крайових обчислень	Так	Так	Так	Так	Так	Так	[67]

Автори [68] досліджували впровадження та тестування передової інфраструктури 5G, поширеної на європейські інформаційно-технологічні ресурси та платформи для перевірки послуг 5G, включно з периферійними обчисленнями з мультидоступом.

2.4 Безпекові проблеми та перспективи подальших досліджень для широкої адаптації периферійних обчислень з мультидоступом в 5G-мережах

Широка адаптація периферійних обчислень з мультидоступом в мережах 5G для реалізації Інтернету речей неминуча. Мережева інфраструктура, стандартизована для 5G, відрізняється від інформаційно-технологічних архітектур та програмно-алгоритмічних застосунків на основі LTE за доступом та формуванням основної мережі. Тому на даний час можна виділити проблеми для реалізації 5G:

– Можливості URLLC обтяжують інженерів безпеки при забезпеченні належного рівня безпеки протоколів зв’язку та накладних витрат корисного обчислювального навантаження.

– Для зменшення накладних витрат потребують дослідження нові криптографічні засоби.

– Масове поширення IoT-застосунків створює обширний перелік проблем використання периферійних ресурсів обробки, зв’язку та мережевих аспектів поширення IoT-пристроями. Очевидно, що керувати безпекою в таких швидкозмінних умовах досить складно.

– Енергоефективність мережевих та крайових вузлів з обмеженими ресурсами є дуже важливою для забезпечення безперервності обслуговування. Тому, механізми енергозбереження та перемикання до сплячих режимів, альтернативні методи збору енергії та оптимальне її використання є дуже важливими для розгортання 5G.

– Міграція послуг стає невід’ємним аспектом периферійних обчислень із локальними обчислювальними засобами на базі мереж 5G-операторів. Необхідно детальныше дослідити пов’язані з процесом міграції проблеми безпеки з точки зору технологій віртуалізації, доменів та обробки на етапі передачі даних.

– Вимоги до масштабованості безпекових рішень є життєво важливими для розгортання периферійних обчислень з мультидоступом на основі 5G, де безпека та часова затримка мають чіткий компроміс. Безпекові функції та механізми повинні застосовуватися комплексно та відповідно до реквізитів із програми та рівнями її пріоритетності.

– На даний час оркестровка є найбільш дослідженим аспектом у сфері віртуалізації. Він вимагає повного автономного контролю з вбудованими засобами на основі штучного інтелекту для периферійних обчислень. Безпека є життєво важливою функцією під час оркестрування. В подальшому її слід стандартизувати для автономної роботи.

Безпека та конфіденційність є життєво важливими вимогами до майбутніх цифрових послуг. Вони мають таке ж значення, як показники продуктивності. Стійкість та захищеність конкретного застосунку до кібервторгнень є вимогливим фактором для підвищення його селективності.

2.5 Висновок до другого розділу

В другому розділі кваліфікаційної роботи подано результати аналізу наукових публікацій про використанням периферійних обчисленнь з мультидоступом в 5G-мережах з точки зору безпеки та конфіденційності систем. Результати аналізу узгоджуються з перспективними прообразами директив, запропонованих в результаті провідних інноваційних досліджень для визначення потенціалу розгортання периферійних обчисленнь з мультидоступом в мережах 5G. Узагальнено потенційні застосування та прогресивні інформаційно-технологічні рішення для інтеграції периферійних обчисленнь з мультидоступом в мережах 5G та підвищення їхнього рівня безпеки.

РОЗДІЛ 3. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

3.1 Шляхи підвищення життєдіяльності людини

Кваліфікаційна робота освітнього рівня «бакалавр» присв'ячена аналіз безпеки периферійних обчисленнь з мультидоступом в мережах 5G. 5G – це назва для позначення у наукових працях та проєктах наступного покоління телекомунікаційних стандартів мобільних мереж після стандартів 4G або «IMT-Advanced». На даний час мобільний зв'язок активно використовується у всіх сферах людського життя та діяльності. Дому доцільно дослідити шляхи підвищення життєдіяльності людини.

Проблема безпеки життєдіяльності (БЖД) людини і всього суспільства в сучасних умовах набула особливої гостроти та актуальності. БЖД обговорюється на сторінках газет і журналів, вченими, представниками громадськості, політичними діячами, тобто є об'єктом уваги всіх прошарків суспільства, громад та держави. Вчені заклопотані небажаними та негативними наслідками антропогенного впливу на природу та навколишнє середовище. Дослідники з різних країн світу розробляють різноманітні моделі майбутнього балансування розвитку людського суспільства з навколишнім середовищем в умовах величезних техногенних навантажень на біосферу [69].

Небезпеки існують у просторі й часі та реалізуються у вигляді потоків енергії, речовини та інформації. Потенційна небезпека стає реальною тоді, коли впливає на фізичні об'єкти. Наприклад, океанський шторм становить небезпеку, якщо в зоні його дії знаходитимуться кораблі. Якщо кораблів немає, то шторм – це просто природнє явище.

Уразливість людини та елементів навколишнього середовища. Уразливість – це незахищеність від небезпеки. Уразливість може бути застосована до окремого елемента системи і всієї системи в цілому.

Для формулювання основних принципів захисту людини доцільно сформулювати множину визначень. Зокрема, гомосфера – це простір, в якому

знаходиться людина в процесі трудової та іншої діяльності і відпочинку. Ноксосфера – простір, у якому постійно існують або можливе виникнення небезпечних чинників [70]. Для реалізації небезпеки необхідне існування перетину гомосфери і ноксосфери. І навпаки – безпека буде забезпечена, якщо гомосфера і ноксосфера не перетинаються.

Розглянемо такі варіанти взаємного розташування гомосфери і ноксосфери (див. рисунок 3.1).

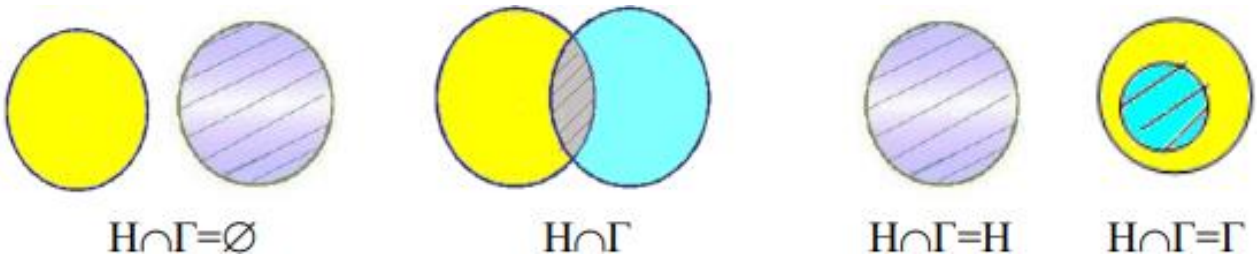

Рисунок 3.1 – Варіанти взаємного розташування гомосфери і ноксосфери

Повну безпеку гарантує лише перший варіант, наприклад, дистанційне керування технологічним процесом. При другому варіанті небезпека існує тільки в місці перетину гомосфери і ноксосфери. Однак, якщо людина знаходиться в такому місці досить короткий час, наприклад, з метою спостереження, проведення планового огляду чи невеликого ремонту. Третій варіант характеризує найбільшу небезпеку, яка може бути реалізована. В четвертому випадку небезпека виникає тільки коли порушено цілісність засобів захисту [70].

Виходячи з можливих варіантів взаємного розташування гомосфери і ноксосфери можна визначити шляхи підвищення безпеки життєдіяльності людини. У процесі формування та експлуатації системи «людина-середовище» доцільно керуватися основними принципами забезпечення безпеки життєдіяльності. Вони повинні відображати комплексний, системний підхід до вирішення міжвідомчих та міжрегіональних проблем. Зокрема:

– розділення гомосфери і ноксосфери у просторі та часі;

– нормалізація ноксосфери – приведення параметрів чинників небезпеки у відповідність до характеристик людини;

– зміна гомосфери – підвищення захисних функцій та властивостей людини завдяки адаптації та застосуванню засобів захисту.

Принципи підвищення рівня життєдіяльності людини дозволяють знаходити оптимальні рішення захисту від небезпек на основі порівняльного аналізу конкуруючих варіантів. Принципи підвищення рівня життєдіяльності людини можуть бути застосовані в різних сферах: техніці, медицині, організації праці та відпочинку [70]. Вони вказують на різноманіття шляхів і методів забезпечення безпеки в системі «людина–середовище», що включають як організаційні заходи, конкретні технічні рішення, так і забезпечення адекватного управління, що гарантує стійкість системи та методологічні положення, що позначають напрямок пошуку рішень.

3.2 Організація ведення робіт в аварійних умовах

На кожному підприємстві мають бути складені плани локалізації та ліквідації аварійних ситуацій і аварій – ПЛАС. Метою плану локалізації і ліквідації аварійних ситуацій і аварій є планування дій (взаємодії) персоналу підприємства, спецпідрозділів, населення, центральних і місцевих органів виконавчої влади та органів місцевого самоврядування щодо локалізації і ліквідації аварій та пом′якшення їх наслідків. Перелік виробництв, зокрема, цехів, відділень, виробничих дільниць і окремих об′єктів, для яких розробляється ПЛАС, визначається і затверджується власником або керівником підприємства. ПЛАС повинен охоплювати всі рівні розвитку аварії, які встановлені в процесі аналізу небезпек [72].

Для забезпечення ефективної боротьби з аварією на всіх рівнях її розвитку наказом створюється штаб, функціями якого є: збір і реєстрація інформації про хід розвитку аварії та вжиті заходи щодо боротьби з нею; поточна оцінка інформації і прийняття рішень щодо оперативних дій в зоні

аварії та поза її межами; координація дій персоналу підприємства і всіх залучених підрозділів і служб, які беруть участь у ліквідації аварії. Загальне керівництво роботою штабу здійснює відповідальний керівник робіт щодо локалізації та ліквідації аварій – ВК. У ПЛАС повинно бути визначене місце розташування штабу, в т.ч. резервне. У ПЛАС повинні бути визначені посадові особи, які виконують функції ВК.

Організація ведення робіт в аварійних умовах під час ліквідації наслідків надзвичайних ситуацій полягає в ефективному керівництві силами цивільного захисту, зокрема оперативно-рятувальною службою цивільного захисту, аварійно-рятувальними службами, формуваннями цивільного захисту, спеціалізованими службами, пожежно-рятувальними підрозділами або частинами, добровільними формуваннями цивільного захисту, при проведенні аварійно-рятувальних та інших невідкладних робіт (АРІНР) [72].

АРІНР – роботи, спрямовані на пошук, рятування і захист населення, уникнення руйнувань і матеріальних збитків, локалізацію зони впливу небезпечних чинників, ліквідацію чинників, що унеможливлюють проведення таких робіт або загрожують життю рятувальників.

Головна мета ведення робіт в аварійних умовах під час ліквідації наслідків надзвичайних ситуацій – забезпечити своєчасне та ефективне виконання завдань у зоні надзвичайної ситуації (НС) у найкоротші терміни та з мінімальними людськими й матеріальними втратами від наслідків НС, наявними ресурсами, зокрема силами та засобами різноманітного призначення для виконання АРІНР [72].

Керівник аварійно-рятувального формування, що прибув у зону НС першим, бере на себе повноваження керівника робіт з ліквідації наслідків НС та виконує їх до прибуття призначеного у встановленому порядку керівника робіт. У випадку технологічної неможливості проведення всього обсягу АРІНР керівник робіт може припинити АРІНР як в цілому, так і за певної їхньої частини, при цьому, в першу чергу, вжити усіх можливих заходів щодо рятування людей, які перебувають у зоні НС.

За гострої необхідності під час організації ведення робіт в аварійних умовах керівник робіт [72] має право самостійно вирішувати питання щодо:

– проведення заходів з евакуації;

– зупинки діяльності організацій, що перебувають у зоні НС;

– проведення АРІНР на об’єктах і територіях організацій, що перебувають у зоні НС;

– обмеження доступу людей у зону НС;

– розбронювання з метою ліквідації наслідків НС резервів матеріальних ресурсів організацій, що перебувають у зоні НС;

– використання у порядку, встановленому законодавством України, засобів зв’язку та транспорту, іншого майна організацій, що перебувають у зоні надзвичайних ситуацій;

– залучення до проведення робіт з ліквідації наслідків НС позаштатних та громадських аварійно-рятувальних формувань, а також рятувальників, що не входять до складу зазначених формувань, за наявності у них документів, що підтверджують їхню атестацію на проведення АРІНР;

– залучення на добровільній основі населення до проведення невідкладних робіт, а також окремих громадян, що не є рятувальниками, з їхньої згоди до проведення АРІНР;

– прийняття інших заходів, обумовлених розвитком НС і ходом робіт з її ліквідації.

3.3 Висновок до третього розділу

В третьому розділі кваліфікаційної роботи описано шляхи підвищення життєдіяльності людини. Розглянуто аспекти організації ведення робіт в аварійних умовах.

ВИСНОВКИ

В першому розділі кваліфікаційної роботи освітнього рівня «Бакалавр» проведено аналіз предметної області та категорій застосунків, зокрема:

– Розглянуто периферійні обчислення з мультидоступом в мережах 5G.

– Зафіксовано стан та перспективи досліджень в галузі.

– Описано безпекові загрози та ризики інноваційних мереж 5G.

– Проаналізовано безпекові загрози та ризики периферійних обчисленнь з мультидоступом.

– Розглянуто категорії застосунків що використовують периферійні обчислення з мультидоступом в мережах 5G.

В другому розділі кваліфікаційної роботи проведено аналіз безпеки периферійних обчислень з мультидоступом в мережах 5G, зокрема:

– Досліджено уразливості безпеки та існуючі рішення для захисту периферійних обчислень з мультидоступом в мережах 5G.

– Подано результати аналізу вразливостей безпеки.

– Висвітлено результати аналізу існуючих рішень щодо запобігання та протидії вразливостям безпеки.

– Описано безпекові проблеми та перспективи подальших досліджень для широкої адаптації периферійних обчислень з мультидоступом в 5G-мережах.

У розділі «Безпека життєдіяльності, основи хорони праці» розглянуто шляхи підвищення життєдіяльності людини. Висвітлено організацію ведення робіт в аварійних умовах.

ПЕРЕЛІК ДЖЕРЕЛ

1 Pete Beckman, Charlie Catlett, Moinuddin Ahmed, Mohammed Alawad, Linquan Bai, Prasanna Balaprakash, Kevin Barker, Pete Beckman, Randall Berry, Arup Bhuyan, et al. 2020. 5G Enabled Energy Innovation: Advanced Wireless Networks for Science, Workshop Report. Technical Report. USDOE Office of Science (SC).

2 Ju Ren, Deyu Zhang, Shiwen He, Yaoxue Zhang, and Tao Li. 2019. A survey on end-edge-cloud orchestrated network computing paradigms: Transparent computing, mobile edge computing, fog computing, and cloudlet. ACM Comput. Surveys 52, 6 (2019), 125.

3 Duda, O., Kunanets, N., Martsenko, S., Matsiuk, O., Pasichnyk, V., Building secure Urban information systems based on IoT technologies. CEUR Workshop Proceedings 2623, pp. 317-328. 2020.

4 Rabia Khan, Pardeep Kumar, Dushantha Nalin K. Jayakody, and Madhusanka Liyanage. 2019. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions. IEEE Commun. Surveys Tutor. 22, 1 (2019), 196–248.

5 Jose Costa-Requena. 2014. SDN integration in LTE mobile backhaul networks. In Proceedings of the International Conference on Information Networking (ICOIN’14). IEEE, 264–269.

6 Hajar Hantouti, Nabil Benamar, Tarik Taleb, and Abdelquoddous Laghrissi. 2018. Traffic steering for service function chaining. IEEE Commun. Surveys Tutor. 21, 1 (2018), 487–507.

7 Chamitha De Alwis, Anshuman Kalla, Quoc-Viet Pham, Pardeep Kumar, Kapal Dev, Won-Joo Hwang, and Madhusanka Liyanage. 2021. Survey on 6G frontiers: Trends, applications, requirements, technologies and future research. IEEE Open J. Commun. Soc. (2021).

8 Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, and Mika Ylianttila. 2018. A Comprehensive Guide to 5G Security. Wiley Online Library.

9 Duda O., Matsiuk O., Kunanets N., Pasichnyk V., Rzheuskyi A., Bilak Y., Formation of Hypercubes Based on Data Obtained from Systems of IoT Devices of Urban Resource Networks, International Journal of Sensors, Wireless Communications and Control (2020) 10: 1. ISSN 2210-3287.

10 Saurabh Singh, Young-Sik Jeong, and Jong Hyuk Park. 2016. A survey on cloud computing security: Issues, threats, and solutions. J. Netw. Comput. Appl. 75 (2016), 200–222.

11 Keke Gai, Meikang Qiu, Hui Zhao, and Jian Xiong. 2016. Privacy-aware adaptive data encryption strategy of big data in cloud computing. In Proceedings of the IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud’16). IEEE, 273–278.

12 Meisong Wang, Prem Prakash Jayaraman, Rajiv Ranjan, Karan Mitra, Miranda Zhang, Eddie Li, Samee Khan, Mukkaddim Pathan, and Dimitrios Georgeakopoulos. 2015. An overview of cloud based content delivery networks: Research dimensions and state-of-the-art. In Transactions on Large-Scale Data-and Knowledge-Centered Systems XX. Springer, 131–158.

13 Pawani Porambage, Jude Okwuibe, Madhusanka Liyanage, Mika Ylianttila, and Tarik Taleb. 2018. Survey on multiaccess edge computing for Internet of Things realization. IEEE Commun. Surveys Tutor. 20, 4 (2018), 2961–2991.

14 Abderrahime Filali, Amine Abouaomar, Soumaya Cherkaoui, Abdellatif Kobbane, and Mohsen Guizani. 2020. Multiaccess edge computing: A survey. IEEE Access 8 (2020), 197017–197046.

15 Mamta Agiwal, Abhishek Roy, and Navrati Saxena. 2016. Next generation 5G wireless networks: A comprehensive survey. IEEE Commun. Surveys Tutor. 18, 3 (2016), 1617–1655.

16 Xenofon Foukas, Georgios Patounas, Ahmed Elmokashfi, and Mahesh K. Marina. 2017. Network slicing in 5G: Survey and challenges. IEEE Commun. Mag. 55, 5 (2017), 94–100.

17 Matthew N. O. Sadiku, Shumon Alam, and Sarhan M. Musa. 2017. Information assurance benefits and challenges: An introduction. Info. Secur. 36, 1 (2017), 1–5.

18 Craig Lee and Andrea Fumagalli. 2019. Internet of Things security-multilayered method for end to end data communications over cellular networks. In Proceedings of the IEEE 5th World Forum on Internet of Things (WF-IoT'19). IEEE, 24–28.

19 Dushantha Nalin K. Jayakody, Kathiravan Srinivasan, and Vishal Sharma. 2019. 5G Enabled Secure Wireless Networks. Springer.

20 Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. 2018. Overview of 5G security challenges and solutions. IEEE Commun. Standards Mag. 2, 1 (2018), 36–43.

21 Madhusanka Liyanage, An Braeken, Pardeep Kumar, and Mika Ylianttila. 2020. IoT Security: Advances in Authentication. John Wiley & Sons.

22 ETSI. 2016. Mobile edge computing (MEC) framework and reference architecture. ETSI White Paper #3. Retrieved from https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_MEC003v010101p.pdf.

23 Ranaweera, Pasika, Anca Jurcut, and Madhusanka Liyanage. "MEC-enabled 5G use cases: a survey on security vulnerabilities and countermeasures." ACM Computing Surveys (CSUR) 54.9 (2021): 1-37.

24 Xi Chen, Zonghang Li, Yupeng Zhang, Ruiming Long, Hongfang Yu, Xiaojiang Du, and Mohsen Guizani. 2018. Reinforcement learning–based QoS/QoE-aware service function chaining in software-driven 5G slices. Trans. Emerg. Telecommun. Technol. 29, 11 (2018), e3477.

25 Yushan Siriwardhana, Pawani Porambage, Mika Ylianttila, and Madhusanka Liyanage. 2020. Performance analysis of local 5G operator architectures for industrial internet. IEEE Internet Things J. 7, 12 (2020), 11559–11575.

26 Duda, O., et al, Selection of Effective Methods of Big Data Analytical Processing in Information Systems of Smart Cities. CEUR Workshop Proceedings 2631, pp. 68-78. 2020.

27 Anca D. Jurcut, Pasika Ranaweera, and Lina Xu. 2020. Introduction to IoT security. In IoT Security: Advances in Authentication. M. Liyanage, A. Braeken, P. Kumar, and M. Ylianttila (Eds.). Wiley. https://doi.org/10.1002/ 9781119527978.ch2.

28 Nasir Abbas, Yan Zhang, Amir Taherkordi, and Tor Skeie. 2018. Mobile edge computing: A survey. IEEE Internet Things J. 5, 1 (2018), 450–465.

29 Kashif Bilal and Aiman Erbad. 2017. Edge computing for interactive media and video streaming. In Proceedings of the 2nd International Conference on Fog and Mobile Edge Computing (FMEC'17). IEEE, 68–73.

30 Shane Fonyi. 2020. Overview of 5G security and vulnerabilities. Cyber Defense Rev. 5, 1 (2020), 117–134.

31 Shuyi Chen, Ruofei Ma, Hsiao-Hwa Chen, Hong Zhang, Weixiao Meng, and Jiamin Liu. 2017. Machine-to-machine communications in ultra-dense Networks–A survey. IEEE Commun. Surveys Tutor. 19, 3 (2017), 1478–1503.

32 Muhammad Usman, Muhammad Rizwan Asghar, Imran Shafique Ansari, and Marwa Qaraqe. 2018. Security in wireless body area networks: From in-body to off-body communications. IEEE Access 6 (2018), 58064–58074.

33 Jonathan Petit and Steven E. Shladover. 2015. Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transport. Syst. 16, 2 (2015), 546–556.

34 Irina Tal and Gabriel-Miro Muntean. 2018. Towards reasoning vehicles: A survey of fuzzy logic-based solutions in vehicular networks. ACM Comput. Surveys 50, 6 (2018), 80.

35 Sahil Garg, Amritpal Singh, Shalini Batra, Neeraj Kumar, and Laurence T. Yang. 2018. UAV-empowered edge computing environment for cyber-threat detection in smart vehicles. IEEE Netw. 32, 3 (2018), 42–51.

36 Jeremy Mitchell, David Soldani, and Malcolm Shore. 2018. The Path to 5G in Australia: Architecture Evolution from 4G to 5G. Retrieved from http://huaweihub.com.au/wp-content/uploads/2018/07/The-path-to-5G-in-Australia-03August-2018-2.pdf.

37 Pasika Ranaweera, Madhusanka Liyanage, and Anca Delia Jurcut. 2020. Novel MEC based approaches for smart hospitals to combat COVID-19 pandemic. IEEE Consum. Electron. Mag. 10, 2 (2020), 80–91.

38 Mohammed S. Elbamby, Cristina Perfecto, Mehdi Bennis, and Klaus Doppler. 2018. Toward low-latency and ultrareliable virtual reality. IEEE Netw. 32, 2 (2018), 78–84.

39 Yuyi Mao, Changsheng You, Jun Zhang, Kaibin Huang, and Khaled B. Letaief. 2017. A survey on mobile edge computing: The communication pserspective. IEEE Commun. Surveys Tutor. 19, 4 (2017), 2322–2358.

40 Daojing He, Sammy Chan, and Mohsen Guizani. 2018. Security in the Internet of Things supported by mobile edge computing. IEEE Commun. Mag. 56, 8 (2018), 56–61.

41 Bin Li, Zesong Fei, and Yan Zhang. 2018. UAV communications for 5G and beyond: Recent advances and future trends. IEEE Internet Things J. 6, 2 (2018), 2241–2263.

42 Vanga Odelu, Ashok Kumar Das, Mohammad Wazid, and Mauro Conti. 2018. Provably secure authenticated key agreement scheme for smart grid. IEEE Trans. Smart Grid 9, 3 (2018), 1900–1910.

43 Keke Gai, Yulu Wu, Liehuang Zhu, Lei Xu, and Yan Zhang. 2019. Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet Things J. 6, 5 (2019), 7992–8004.

44 Mohammad Borhani, Madhusanka Liyanage, Ali Hassan Sodhro, Pardeep Kumar, Anca Delia Jurcut, and Andrei Gurtov. 2020. Secure and resilient communications in the industrial internet. In Guide to Disaster-Resilient Communication Networks. Springer, 219–242.

45 Arash Nourian and Stuart Madnick. 2018. A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet. IEEE Trans. Depend. Secure Comput. 15, 1 (2018), 2–13.

46 Chiking Lee. 2018. Discovering cyber vulnerabilities in SCADA control system via examination of water treatment plant in laboratory environment. UNSW Canberra ADFA J. Undergrad. Eng. Res. 9, 1 (2018).

47 Syed Noorulhassan Shirazi, Antonios Gouglidis, Kanza Noor Syeda, Steven Simpson, Andreas Mauthe, Ioannis M. Stephanakis, and David Hutchison. 2016. Evaluation of anomaly detection techniques for SCADA communication resilience. In Proceedings of the Resilience Week (RWS'16). IEEE, 140–145.

48 Razin Farhan Hussain, Mohsen Amini Salehi, Anna Kovalenko, Saeed Salehi, and Omid Semiari. 2018. Robust resource allocation using edge computing for smart oil fields. In Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'18). The Steering Committee of The World Congress in Computer Science, 204–210.

49 Helen C. Leligou, Theodore Zahariadis, Lambros Sarakis, Eleftherios Tsampasis, Artemis Voulkidis, and Terpsichori E. Velivassaki. 2018. Smart grid: A demanding use case for 5G technologies. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom'18). IEEE, 215–220.

50 Michael Langfinger, Michael Schneider, Didier Stricker, and Hans D. Schotten. 2017. Addressing security challenges in industrial augmented reality systems. In Proceedings of the 15th International Conference on Industrial Informatics (INDIN'17). IEEE, 299–304.

51 Olli Mäkinen. 2015. Streaming at the edge: Local service concepts utilizing mobile edge computing. In Proceedings of the 9th International Conference on Next Generation Mobile Applications, Services and Technologies. IEEE, 1–6.

52 Miguel Saez, Steven Lengieza, Francisco Maturana, Kira Barton, and Dawn Tilbury. 2018. A data transformation adapter for smart manufacturing systems

with edge and cloud computing capabilities. In Proceedings of the IEEE International Conference on Electro/Information Technology (EIT'18). IEEE, 0519–0524.

53 Meng Li, Richard Yu, Pengbo Si, and Yanhua Zhang. 2018. Energy-efficient machine-to-machine (M2M) communications in virtualized cellular networks with mobile edge computing (MEC). IEEE Trans. Mobile Comput. 18, 7 (2018), 1541–1555.

54 Xi Zhang and Qixuan Zhu. 2017. Statistical quality of service provisioning over edge computing mobile wireless networks. In Proceedings of the IEEE Military Communications Conference (MILCOM'17). IEEE, 412–417.

55 Lijun Dong and Guoqiang Wang. 2017. Information centric approach in achieving anycast service in machine type communications. In Proceedings of the IEEE Conference on Standards for Communications and Networking (CSCN'17). IEEE, 157–162.

56 An Braeken, Pawani Porambage, Amirthan Puvaneswaran, and Madhusanka Liyanage. 2020. ESSMAR: Edge supportive secure mobile augmented reality architecture for healthcare. In Proceedings of the 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech'20). IEEE, 1–7.

57 Simon Parkinson, Paul Ward, Kyle Wilson, and Jonathan Miller. 2017. Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE Trans. Intell. Transport. Syst. 18, 11 (2017), 2898–2915.

58 Shankar Lal, Tarik Taleb, and Ashutosh Dutta. 2017. NFV: Security threats and best practices. IEEE Commun. Mag. 55, 8 (2017), 211–217.

59 Muhammad Javed, Elyes Ben Hamida, Ala Al-Fuqaha, and Bharat Bhargava. 2017. Adaptive security for intelligent transport system applications. IEEE Intell. Transport. Syst. Mag. 10, 2 (2017), 110–120.

60 Dennis Grewe, Marco Wagner, Mayutan Arumaithurai, Ioannis Psaras, and Dirk Kutscher. 2017. Information-centric mobile edge computing for connected vehicle environments: Challenges and research directions. In Proceedings of the Workshop on Mobile Edge Communications. ACM, 7–12.

61 Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards security and privacy for multi-user augmented reality: Foundations with end users. In Proceedings of the IEEE Symposium on Security and Privacy (SP'18). IEEE.

62 Xiuquan Qiao, Pei Ren, Schahram Dustdar, and Junliang Chen. 2018. A new era for web AR with mobile edge computing. IEEE Internet Comput. 22, 4 (2018), 46–55.

63 Reham M. Fouda. 2018. Security vulnerabilities of cyberphysical unmanned aircraft systems. IEEE Aerospace Electronic Syst. Mag. 33, 9 (2018), 4.

64 Archana Rajakaruna, Ahsan Manzoor, Pawani Porambage, Madhusanka Liyanage, Mika Ylianttila, and Andrei Gurtov. 2019. Enabling end-to-end secure connectivity for low-power IoT devices with uavs. In Proceedings of the IEEE Wireless Communications and Networking Conference Workshop (WCNCW'19). IEEE, 1–6.

65 Michael Hooper, Yifan Tian, Runxuan Zhou, Bin Cao, Adrian P. Lauf, Lanier Watkins, William H. Robinson, and Wlajimir Alexis. 2016. Securing commercial wifi-based UAVs from common security attacks. In Proceedings of the Military Communications Conference (MILCOM'16). IEEE, 1213–1218.

66 Neeraj Kumar, Sherali Zeadally, and Joel J. P. C. Rodrigues. 2016. Vehicular delay-tolerant networks for smart grid data management using mobile edge computing. IEEE Commun. Mag. 54, 10 (2016), 60–66.

67 Pasika Ranaweera, Vashish N. Imrith, Madhusanka Liyanag, and Anca Delia Jurcut. 2020. Security as a service platform leveraging multi-access edge computing infrastructure provisions. In Proceedings of the IEEE International Conference on Communications (ICC'20). IEEE, 1–6.

68 EU-H2020. 2018. 5G-EVE. Retrieved from https://www.5g-eve.eu/.

69 Толок А.О. Крюковська О.А. Безпека життєдіяльності: Навч. посібник. – 2011. – 215 с.

70 Стиценко Т.Є., Пронюк Г.В., Сердюк Н.М., Хондак І.І. «Безпека життєдіяльності»: навч. посібник / Т.Є Стиценко, Г.В. Пронюк, Н.М. Сердюк, І.І. Хондак. – Харків: ХНУРЕ, 2018. – 336 с.

71 У Держпраці розповіли про організацію роботи на виробництвах з підвищеною небезпекою під час воєнного стану. URL: https://www.sop.com.ua/news/3476-u-derjprats-rozpovli-pro-organzatsyu-roboti-na-virobnitstvah-z-pdvishchenoyu-nebezpekoyu-pd.

72 Основи організації й проведення аварійно-рятувальних та інших невідкладних робіт під час ліквідації надзвичайної ситуації. Спецкурс. Цивільний захист. URL: https://ns-plus.com.ua/2019/06/10/osnovy-organizatsiyi-j-provedennya-avarijno-ryatuvalnyh-ta-inshyh-nevidkladnyh-robit-pid-chas-likvidatsiyi-nadzvychajnoyi-sytuatsiyi/.