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: Методи інтелектуального аналізу даних для виявлення кіберзагроз у «розумних містах»

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

_____ Базан І.В.
(підпис) (прізвище та ініціали)

Керівник _____ Матійчук Л.П.
(підпис) (прізвище та ініціали)

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

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

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Тернопіль
2023

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)
«25» _грудня 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 124 Системний аналіз
(шифр і назва спеціальності)

Студенту Базан Ірина Володимирівна
(прізвище, ім'я, по батькові)

1. Тема роботи Методи інтелектуального аналізу даних для виявлення кіберзагроз у «розумних містах»

Керівник роботи Матійчук Любомир Павлович, к.е.н., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 24 » листопада 2023 року № 4/7-1096

2. Термін подання студентом завершеної роботи 28 грудня 2023р.

3. Вихідні дані до роботи Наукові публікації про інтелектуального аналізу даних для виявлення кіберзагроз,

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 Аналіз предметної області. 1.1 Архітектура «розумного міста». 1.2 Кібер-загрози для «розумного міста». 1.2.1 Розвідувальні загрози. 1.2.2 Диверсії інфраструктури. 1.2.3 Маніпуляції з даними. 1.2.4 Сторонні вразливості. 1.3 Висновок до першого розділу. 2 Категорії, методи та моделі виявлення кіберзагроз. 2.1 Моделі взаємозалежності. 2.2 оцінка ризиків та розвідка загроз. 2.3 Методи виявлення атак. 2.4 Теоретичне підгрунтя. 2.4.1 Машинне навчання та методи аналізу даних. 2.5 Візуальний супровід. 2.6 Вихідні дані: введення, інтерпретація та набори даних. 2.7 Показники порівняння та оцінки моделей. 2.7.1 Моделі взаємозалежності. 2.7.2 Методи оцінки ризиків. 2.7.3 Методи виявлення атак. 2.8 Відкриті питання та виклики. 2.9 Висновок до другого розвитку. 3 Реалізація запропонованої моделі. 3.1 Згорткова нейронна мережа. 3.2 Квазіконкурентна нейронна мережа. 3.3 Запропонована гібридна модель DL для кіберзагроз. 3.4 Набори даних. 3.5 Попередня обробка даних. 3.6 Реалізація моделі. 3.7 Інструменти та показники оцінювання 3.8 Оцінка та аналіз. 3.9 Висновок до третього розділу. 4 Охорона праці та безпека в надзвичайних ситуаціях. 4.1 Питання щодо охорони праці. 4.2 Питання щодо безпеки в надзвичайних ситуаціях.4.3 Висновок до четвертого розділу. Висновки. Додатки

5. Перелік графічного матеріалу 1 Титульна сторінка. 2 Тема, Мета, Об'єкт, Предмет дослідження. 3 Завдання дослідження. 4 Актуальність дослідження. 5 Масштаб дослідження. 6 Високорівнева архітектура «розумних міст». 7 Ландшафт загроз. 8 Розвідувальні загрози. 9 Диверсії інфраструктури. 10 Маніпуляції даними. 11 Сторонні вразливості. 12 Класи моделей. 13.Архітектура гібридної моделі. 14 Набір даних Bot-IoT. 15 Набір даних TON_IoT. 16 Висновки. 17 Завершальний слайд.

6. Консультанти розділів роботи

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

7. Дата видачі завдання 24 листопада 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	25.11.2023	*Виконано*
2.	Підбір наукових джерел про методи інтелектуального	26.11.2023-28.11.2023	*Виконано*
	аналізу даних для виявлення кіберзагроз у «розумних		
	містах»		
3.	Опрацювання наукових публікацій та збір даних по	29.11.2023-1.12.2023	*Виконано*
	темі роботи		
4.	Виконання дослідження згідно мети кваліфікаційної	2.12.2023-4.12.2023	*Виконано*
	роботи		
5.	Оформлення розділу «Аналіз предметної області»	5.12.2023-7.12.2023	*Виконано*
6.	Оформлення розділу «категорії, методи та моделі	8.12.2023-10.12.2023	*Виконано*
	Виявлення кіберзагроз»		
7.	Оформлення розділу «Реалізація запропонованої	11.12.2023-13.12.2023	*Виконано*
	моделі»		
8.	Виконання завдання до підрозділу «Охорона праці»	14.12.2023-15.12.2023	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в	16.12.2023-17.12.2023	*Виконано*
	надзвичайних ситуаціях»		
10.	Оформлення кваліфікаційної роботи	18.12.2023-19.12.2023	*Виконано*
11.	Нормоконтроль	19.12.2023-20.12.2023	*Виконано*
12.	Перевірка на плагіат	21.12.2023	*Виконано*
13.	Попередній захист кваліфікаційної роботи	22.12.2023	*Виконано*
14.	Захист кваліфікаційної роботи	28.12.2023	

Студент _____ Базан І.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Матійчук Л.П.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи інтелектуального аналізу даних для виявлення кіберзагроз у «розумних містах» // Кваліфікаційна робота освітнього рівня «Магістр» // Базан Ірина Володимирівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група САм-61 // Тернопіль, 2023 // С. 85, рис. – 15, табл. – 8, кресл. – 17, додат. – 2, бібліогр. – 123.

Ключові слова: розумне місто, безпека, загроза, кібераналітика, машинне навчання, глибоке навчання, прийняття рішень

Кваліфікаційна робота присв'ячена розробці інтелектуальних методів аналізу даних для виявлення та протидії кіберзагрозам у «розумних містах».

В першому розділі кваліфікаційної роботи описано архітектуру «розумного міста», висвітлено кіберзагрози для «розумного міста»

В другому розділі кваліфікаційної роботи описано моделі взаємозалежності та оцінку ризиків загроз, досліджено методи виявлення атак, подано порівняльний опис показників порівняння та оцінки моделей.

В третьому розділі кваліфікаційної роботи запропонована реалізація гібридної моделі виявлення кіберзагроз, протестовано квазіконкурентну нейронну мережу, подано відповідні набори даних та їх реалізованої їх обробку.

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

ANNOTATION

Data mining methods for cyber threats detecting in "Smart cities" // The educational level "Master" qualification work // Bazan Iryna Volodymyrivna // Ternopil Ivan Pulyuy National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, SAm-61 group // Ternopil, 2023 // P. 85, fig. - 15, tables - 8, posters - 17, annexes - 2, ref. - 123.

Key words: smart city, security, threat, cyber analytics, machine learning, deep learning, decision-making

The qualification work is devoted to the development of intelligent data analysis methods for detecting and counteracting cyber threats in smart cities.

The first section of the qualification work describes the architecture of the "smart city", highlights the cyber threats to the "smart city"

The second section of the qualification work describes interdependence models and threat risk assessment, examines attack detection methods, and provides a comparative description of the indicators for comparing and evaluating models.

The third section of the qualification work proposes the implementation of a hybrid model for detecting cyber threats, tests a quasi-competitive neural network, presents the relevant data sets and their implemented processing.

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

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

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

DDoS attack (англ. англ. Distributed denial-of-service attack) – розподілена атака на відмову в обслуговуванні

API (англ. application programming interface) – Прикладний програмний інтерфейс.

KNN method (англ. k-nearest neighbor method) – Метод k-найближчих сусідів

DL (англ. deep learning) – Глибоке навчання.

DTW (англ. dynamic time warping) – Алгоритм динамічної зміни часу.

Random forest (англ. Internet of Things) – Інтернет речей.

КІ – критична інфраструктура

КФС – кіберфізична система

CNN (англ. convolutional neural network) – Згорткова нейронна мережа.

RNN (англ. recurrent neural networks) – Рекурентна нейронна мережа

ЗМІСТ

ВСТУП

Актуальність теми. Зростання технологічного прогресу та впровадження концепції «розумних міст» перетворює сучасні міста в складний екосистемний інформаційний простір. Однак разом з перевагами цього розвитку з'являються серйозні загрози кібербезпеці, які можуть значно вплинути на безпеку та життєзабезпечення мешканців міст. Зокрема, зростаюча кількість підключених пристроїв та систем у "розумних містах" створює ідеальне середовище для кіберзлочинців та державно-санкціонованих атак. Завдання забезпечення кібербезпеки в «розумних містах» стає більш актуальним і важливим, оскільки від цього залежить якість життя мешканців та стабільність міського середовища. З урахуванням стрімко зростаючого обсягу збираної та оброблюваної інформації, важливо вдосконалювати та пристосовувати методи захисту для виявлення та вразливостей до нових форм кіберзагроз, щоб убезпечити міста від можливих загроз та атак.

Таким чином, дослідження з кібербезпеки в "розумних містах" визначається як стратегічно важливе і докладне розглядання цієї теми стає невід'ємною частиною розвитку сучасного суспільства та технологічної еволюції міського середовища.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є підвищення рівня повноти подання інформації щодо аналізу та класифікації кіберзагроз у контексті «розумних міст», визначення стійкості різних методів захисту та розробка нових підходів для забезпечення кібербезпеки. Для досягнення поставленої мети потрібно виконати ряд завдань, зокрема:

– Проаналізувати стан досліджень в області існуючих методів виявлення кіберзагроз.

– Дослідити існуючі функціональні архітектури міст.

– Проаналізувати методи виявлення атак.

– Виконати порівняння інструментів та методів оцінок кіберзагроз.

– Розробити модель виявлення кіберзагроз.

Об’єкт дослідження є системи інтелектуального аналізу даних, які використовуються в розумних містах для виявлення та протидії кіберзагрозам.

Предмет дослідження. методи і технології інтелектуального аналізу даних, спрямовані на виявлення кіберзагроз у «розумних містах».

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що отримала подальший розвиток модель інтелектуального аналізу даних для виявлення кіберзагроз у «розумних містах»

Практичне значення одержаних результатів. Дослідження надає практичну вартість для розробників систем «розумних міст» та органів управління.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на IX науково-технічної конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (м. Тернопіль, 2023 р.).

Публікації. Основні результати кваліфікаційної роботи опубліковано у двох працях конференції (Див. додаток А).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури з 123 найменувань та 1 додатку. Загальний обсяг кваліфікаційної роботи складає 85 сторінки, з них 68 сторінки основного тексту, який містить 15 рисунків та 8 таблиць.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

За прогнозами Організації Об'єднаних Націй, до 2050 року дві третини населення світу проживатимуть у містах [1]; це означає, що близько 1,5 мільйона людей по всьому світу переїжджатимуть до міста щотижня [2]. Таке стрімке зростання супроводжується безліччю викликів і можливостей. Фактично, ми є свідками інтенсивного розвитку нової інфраструктури для підтримки такої великої кількості населення в досягненні їхніх екологічних, соціальних та економічних цілей. Від покращення умов дорожнього руху до оптимізації енергоспоживання - розумні міста підвищують якість життя своїх мешканців, зменшуючи викиди вуглекислого газу та оптимізуючи витрати на комунальні послуги.

Завдяки впровадженню новітніх технологій - від телекомунікаційних засобів до досягнень у сфері штучного інтелекту на основі даних - муніципальна інфраструктура, підключена до Інтернету, паркомати тощо продовжують збирати та аналізувати дані для підтримки прийняття рішень і виявлення недоліків для оптимізації в режимі реального часу. Наприклад, міста досягають значного скорочення витрат на опалення, вентиляцію та кондиціонування повітря, встановлюючи системи охолодження на основі Інтернету речей (IoT) для оптимізації на основі активності в кожній кімнаті [3]. Крім того, «розумна» мережа безпосередньо пов'язана з ресурсоефективними рішеннями забезпечення, які підтримують цілі сталого розвитку «розумних міст». Більше того, технології, що розвиваються, завдяки досягненням у сфері поверхневого та глибинного навчання, аналізують закономірності споживання енергії в масштабах міста, щоб постачати лише оптимальну кількість енергії. Крім того, міста використовують давачі для виявлення витоків у трубах; Нью-Йорк заощадив понад 73 мільйони доларів на витратах на воду, повідомляючи мешканців про можливі (прогнозовані) витоки води [4]. Останнє стало можливим після впровадження «розумних» лічильників води та завдяки використанню передових алгоритмів аналізу даних. Крім того, розумні міста продовжують підтримувати безпеку своїх громадян. Так, завдяки використанню

системи підключених відеоканалів місто Ріо-де-Жанейро покращило час реагування на надзвичайні ситуації [5], а Чикаго знизило рівень насильницьких злочинів завдяки використанню предиктивних теплових карт злочинності, що допомагають поліції [6].

Розумні міста виходять за рамки підключеної інфраструктури, залучаючи і перетворюючи громадян, туристів і бізнес-організації в інтелектуальну екосистему шляхом стимулювання інновацій [2]. Поступово міські адміністрації надають дані кінцевим користувачам, намагаючись підтримати прийняття кращих рішень, створюючи рішення для міських проблем, при цьому позитивно змінюючи основну діяльність міста.

З огляду на стрімке зростання «розумних міст» у всьому світі, інтуїтивно зрозуміло і важливо визнати виснажливий і руйнівний вплив кібератак на ці ініціативи. Наприклад, атака, яка завадила авіадиспетчерам шведського аеропорту відстежувати літаки на своїх радарах [7], могла призвести до катастрофічних наслідків. Більш того, ефект очевидний у випадку атаки на електромережу, яка залишила без світла майже 225 000 людей у трьох областях України [8]. Крім того, зловмисні дії вірусу-здирника тимчасово вивели з ладу кілька критично важливих служб міста Атланта, що призвело до перебоїв у роботі комунальних систем та інших ключових служб [9]. Місто Балтимор не тільки втратило незамінні дані, пов'язані з правоохоронною діяльністю, а й зазнало атаки вірусу-здирника на службу екстреної допомоги, що призвело до зриву операції з надання екстреної допомоги [10]. Даллас зазнав лиха через відсутність кіберстійких пристроїв Інтернету речей, що дозволило хакерам порушити належну роботу дорожніх знаків [11] та увімкнути сирени оповіщення посеред ночі [12]. Такі інциденти, як і багато інших, підривають довіру до «розумних міст», перешкоджаючи реалізації їхнього повного потенціалу. Тому вкрай важливо продовжувати розглядати і досліджувати кіберзагрози «розумних міст».

Дійсно, нові вразливості, що з'явилися в результаті злиття технологічних досягнень, а також складність, анонімність і серйозність кіберзагроз створюють нові виклики для прийняття рішень, пов'язаних з кіберпростором. Слід

зазначити, що стандарти і методології кібербезпеки традиційних систем інформаційних технологій не можуть бути безпосередньо застосовані до екосистеми «розумного міста». Це видно на багатьох нещодавніх прикладах. Ховаючись за хмарою, зловмисники використовували алгоритми машинного навчання та експлуатували нові технології, що розвиваються, такі як IoT з підтримкою 5G, щоб посилити можливості атаки [13], а отже, і вплив. Більше того, складність взаємодії між багатьма компонентами інфраструктури експоненціально збільшує вплив кібератак. Застарілі системи виявлення аномалій не встигають за швидким розвитком атак, а жадібні до даних методи, які використовують ознаки зловмисності для виявлення атак, продовжують відставати від них. Природно, що сучасні дослідницькі тенденції вказують на використання підходів до кібербезпеки, заснованих на аналітиці [14, 15]. Наприклад, машинне навчання (в тому числі глибоке навчання) швидко стає ключовим інструментом кібербезпеки, оскільки воно намагається ефективно і семантично інтегрувати і обробляти різні джерела інформації.

Захист «розумних міст» від кібератак є ключовим завданням для їхнього виживання. Хоча кібербезпека є одним з ключових викликів для «розумних міст», вивчення кіберзагроз є досить складним завданням через складність архітектури «розумного міста», його суперечливі вимоги до безпеки та використання широкого (вразливого) програмного забезпечення. Проаналізуємо три групи методів, класифікованих на рис. 1.1.

По-перше, щоб з'ясувати, як загрози впливають на всю екосистему, варто вивчити методи, які моделюють залежності між компонентами розумних міст. По-друге, дослідити методи оцінки ризиків та контекстну розвідку загроз (які дозволяють характеризувати та передбачати просунуті та скоординовані загрози), оцінюючи їхні можливості та наслідки. І також розглянути методи виявлення атак, які допомагають оперативно реагувати на загрози, сприяючи ретроспективному цифровому аналізу, а отже, забезпечують ситуаційну обізнаність і можливість визначення пріоритетів загроз.

Зокрема, в даній роботі порівнюється і протиставляється, а також обговорюється кожен метод виявлення відповідно до наступних критеріїв:

- Теоретичне підґрунтя

- Введення даних та використаний набір даних

- Метрики оцінки точності та продуктивності

- Масштаб

- Підтримка візуальних засобів

Виходячи з цих міркувань, сформулюємо дослідження наступним чином:

Рисунок 1.1 – Масштаб дослідження

А саме:

- Класифікуємо та перераховуємо загрози, спрямовані на архітектуру розумних міст, пов'язуємо відповідні атаки та окреслюємо вплив таких загроз на функціонування розумних міст.

- Описуємо методи, які були розроблені для підтримки кіберситуаційної обізнаності в контексті «розумних міст». З цією метою розглянемо три групи методів: моделі взаємозалежності, оцінка ризиків і вразливостей та виявлення атак.

- Щоб запропонувати новий погляд на методи, що підтримують ситуаційну обізнаність, важливо розуміти їх теоретичне підґрунтя, пов'язати наявні методи з відповідними ідентифікованими загрозами та оцінити візуальну підтримку відповідних методів.

- Щоб уможливити і мотивувати відтворювані методи дослідження, сформуємо фундаментальні характеристики використаних наборів даних, які застосовуються для цілей оцінки. Крім того, порівнюється ефективність використовуваних в даний час показників ефективності, пропонуючи кілька додаткових індикаторів.

Зростання кількості «розумних міст» у всьому світі привернуло величезну увагу дослідницької спільноти. Щоб висвітлити проблеми та напрямки досліджень у контексті кібербезпеки розумних міст, було опубліковано значну кількість оглядів щодо викликів та останніх дослідницьких тенденцій. Хоча деякі теми в дослідженнях перетинаються, рівень деталізації та точки зору варіюються.

Застосування смарт-технологій та методологій використання даних дозволило розробити численні рішення для ключових проблем міст (зокрема, швидкої урбанізації, зростання злочинності, зміни клімату тощо). Щоб проілюструвати еволюцію «розумних міст», ряд авторів продемонстрували технологічні досягнення, надаючи загальний опис [16-18] та конкретні приклади впровадження [17, 19-21]. Основна увага в цих статтях була зосереджена на тому, щоб проілюструвати технологічний прогрес і важливість взаємодії між соціальними і технічними системами. Насправді, ця взаємодія відіграє критично важливу роль у вирішенні міських проблем і підтримці інновацій та підприємництва.

Кілька інших робіт запропонували функціональну архітектуру для розумних міст, визначивши і розчленувавши фізичний, комунікаційний, інформаційний та прикладний рівні. Помітний певний рівень розбіжностей у тому, як автори компілюють ці шари. Наприклад, рівень даних не визнається в [22] або представлений як один [18] чи два [21] екземпляри. Дивно, але жодна з цих архітектур не згадує про рівень управління, який відповідає за управління активами, надання послуг та безпеку.

Будь-яке обговорення «розумного» міського розвитку повинно починатися з вивчення інфраструктури та технологій, що її забезпечують. З цією метою багато дослідників працювали над приводами, сенсорними мережами, Інтернетом речей, спеціальними мережами для транспортних засобів (VANET), мобільними спеціальними мережами (MANET), а також мережами доступу та передачі даних [16-18]. Наприклад, мережі передачі даних можуть бути використані для підтримки кращого прийняття рішень і розподілу ресурсів для «розумних» мереж, управління водними ресурсами та відходами, безпеки,

вирішення надзвичайних ситуацій і багато чого іншого шляхом забезпечення передачі даних. Фактично, дані, що використовуються для передачі, вже збираються з навколишнього середовища різними давачами.

Крім того, складні взаємозалежні відносини між окремими об'єктами критичної інфраструктури відіграють значну роль у розвитку розумних міст. Однак, здається, що багато наявних моделей не здатні охопити таку складну взаємозалежність, щоб зрозуміти весь спектр навмисних і випадкових загроз [23, 24].

Крім того, гетерогенність, обмежені обчислювальні можливості, розподілене розташування та застаріла інфраструктура привертають увагу до загроз та вимог кібербезпеки. Не дивно, що атаки, спрямовані на технології «розумних» міст, отримали переважну увагу [16-19, 21, 25-27]. Дійсно, вимоги та стандарти є ключовими факторами, які визначають необхідний рівень кіберзахисту та пріоритетність загроз. Насправді, надійна автентифікація, безпечний зв'язок, захист даних, моніторинг і виправлення помилок є одними з основних обговорюваних вимог і контрзаходів [16, 17, 20, 21, 25-27], які передбачалися для захисту «розумних міст» від супротивників.

1.1 Архітектура «розумного міста»

Міська інфраструктура інтегрує та поглинає швидкі технологічні досягнення, такі як цифрові дані та інтелектуальна аналітика, що забезпечує кращі послуги для громадян, покращує якість життя та зменшує шкоду навколишньому середовищу. Хоча включення цих елементів залежить від стратегії розвитку та рівня впровадження в конкретних містах, доцільно обєднати прогрес впровадження 10 «розумних міст», щоб змоделювати архітектуру на різних операційних рівнях.

Міська інфраструктура складається з кіберсистем, інтегрованих у фізичні компоненти в різних середовищах, і включає в себе критично важливу інфраструктуру, таку як енергетика, транспорт, державне управління тощо. Проаналізувавши різноманітні тематичні дослідження [2], можна виділити 5

рівнів архітектури розумного міста, а саме: фізичний світ, засоби, дані, додатки та рівень управління. Для повноти картини в проілюстрованій архітектурі ми розглядаємо зацікавлені сторони як постачальників і споживачів.

Рисунок 2 надає візуальне представлення архітектури розумного міста разом з її 5 рівнями.

Рівень фізичного світу охоплює міську інфраструктуру і представляє будівлі, автомобілі, дороги, мости і вуличні ліхтарі, серед іншого.

Рівень реалізації складається з апаратного забезпечення та комунікаційних технологій, які дозволяють збирати дані з навколишнього середовища та передавати їх на наступний архітектурний рівень. Фактично, апаратне забезпечення може складатися з різних типів датчиків, пристроїв або віртуальних машин. Крім того, різні протоколи, включаючи IEEE 802.15.4, IEEE 802.15.4g, Bluetooth, LoRsa, LoRaWAN, розширюють можливості датчиків для курації та збору даних, щоб вони могли передавати інформацію на рівень даних.

Рівень даних - це серце розумних міст. Він складається з величезного обсягу неструктурованих даних, які повинні бути зібрані і належним чином збережені, щоб забезпечити відкритий доступ і застосування численних алгоритмів для кращого прийняття рішень. Власне, штучний інтелект (і ширше - методи навчання) є одними з найпопулярніших методів на цьому рівні. Останній також відповідає за розміщення даних у візуальному контексті, щоб уможливити розуміння значущості даних та покращити процес нагляду. Крім того, цей рівень відповідає за обмін даними між власниками даних, постачальниками послуг і користувачами, пропонуючи платформи відкритих даних.

Рівень застосунків представляє різноманітні комплексні рішення, які «розумні міста» надають своїм клієнтам. Наприклад, транспортні системи на основі даних вирішують проблеми заторів і забруднення, керують паркуванням і громадським транспортом, підвищують безпеку дорожнього руху і покращують графіки перевезень. З цією метою ці рішення інтегрують дані з різних джерел, таких як географічно розподілені давачі руху і погоди, камери і GPS, для застосування алгоритмічного аналізу, пропонуючи оптимальні маршрути. Крім того, впровадження підтримуваних пристроїв Інтернету речей долає обмеження

традиційних систем моніторингу. Так, давачі збирають різні екологічні вимірювання, такі як рівень забруднення повітря або хімічний склад води, тоді як інтелектуальні платформи корелюють отримані дані, щоб адаптувати попередження або уникнути екологічних катастроф. Крім того, новітні розробки в галузі електромереж дозволяють споживачеві відстежувати споживання електроенергії в режимі реального часу. Це підвищує надійність передачі електроенергії, оптимізує необхідний рівень постачання та мінімізує витрати на споживання. Крім того, керована даними система будівлі обробляє та реагує на навколишні зміни, автоматично перемикаючи кондиціонери на основі прогнозів погоди або вимірювань навколишнього середовища. Це лише кілька рішень, які надають розумні міста.

Останній рівень, а саме рівень управління, займається наданням послуг, управлінням активами та безпекою. Зазначимо, що управління рішеннями розумних міст може бути як централізованим, так і децентралізованим. На рисунку 1.2 подано високорівневу архітектуру «розумних міст» з різними операційними рівнями

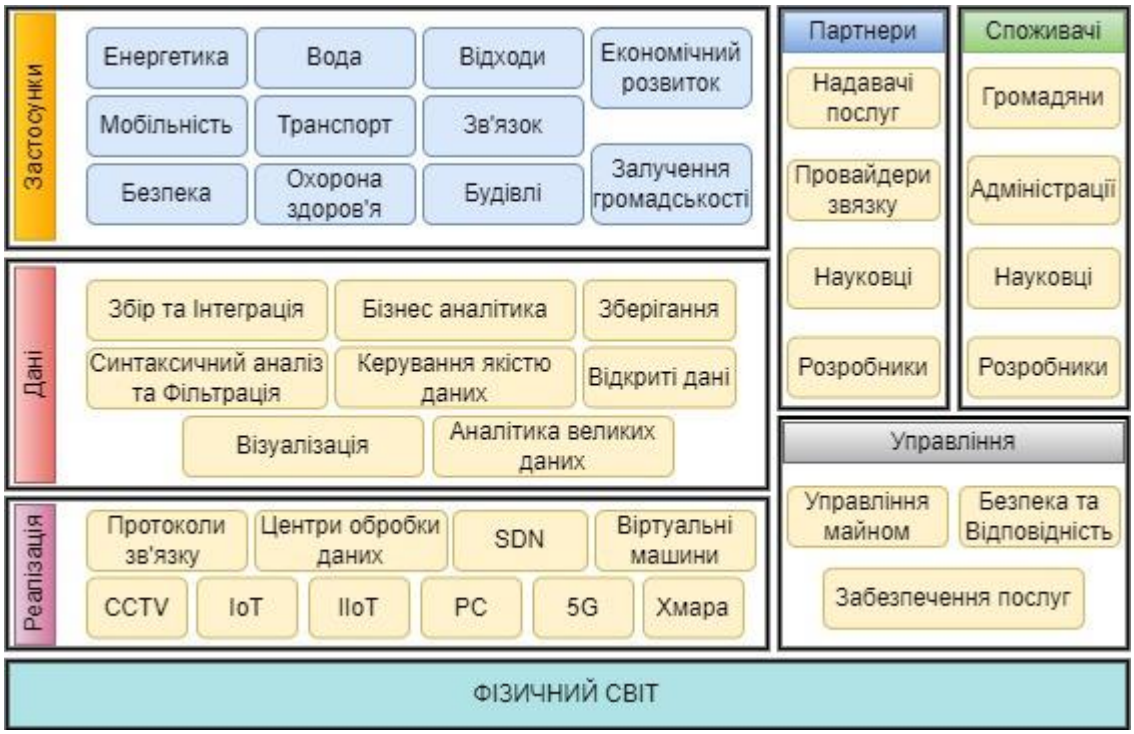

Рисунок 1.2 – Високорівнева архітектура «розумних міст» з різними операційними рівнями

1.2 Кібер-загрози для «розумного міста»

Постійний технологічний розвиток, однак, відкрив нові можливості для кіберзлочинців скористатися вразливістю міст. Міста по всьому світу продовжують ставати жертвами кіберзлочинів, таких як хакерські атаки, програми-вимагачі, крадіжки комунальних послуг та втрата контролю над інфраструктурою. Передбачувано, що безпека стає дуже важливим викликом для розумних міст [28]. Дійсно, є кілька причин, чому впровадження кібербезпеки в умовах «розумних міст» є досить складним завданням, включаючи неоднорідність і географічний розподіл інфраструктури, труднощі з виправленнями, часто обмежені обчислювальні можливості розподілених пристроїв, використання застарілого обладнання, труднощі з вимірюванням безпеки і конфіденційності, а також неузгодженість вимог до забезпечення безпеки.

Хоча загрози залежать від рівня розвитку та архітектури конкретного «розумного міста», розглянемо найпоширеніші загрози, націлені на «розумні» міста. Зверніть увагу, що ми виключили з цього дослідження такі загрози, як збій апаратного забезпечення, програмні та людські помилки, а також перебої в електропостачанні.

По-перше, клас «розвідувальних загроз» складається з загроз, що мають на меті перерахувати ресурси та облікові дані. По-друге, «диверсії інфраструктури» - це загрози, спрямовані на знищення або отримання контролю над інфраструктурою розумного міста шляхом розгортання шкідливого програмного забезпечення і перепрограмування або перевантаження основних ресурсів. По-третє, клас «маніпуляції з даними» складається із загроз, які намагаються підірвати конфіденційність і цілісність даних, а також дестабілізувати алгоритми машинного навчання. Нарешті, «сторонні вразливості» - це загрози, спрямовані на постачальників послуг, які мають значний вплив на діяльність і безпеку «розумних міст».

Рисунок 1.3 – Ландшафт загроз «розумних міст»

Смарт-технології широко використовуються в критично важливих секторах інфраструктури для надання цінних послуг споживачам. Тому вкрай важливо усвідомлювати, як виявлені загрози ставлять під загрозу безперервність діяльності «розумних міст». Ландшафт загроз для «розумних міст» наведено на рисунку 1.3. Однак брак доступу до даних про інциденти в режимі реального часу ускладнює кількісну оцінку такого впливу.

1.2.1 Розвідувальні загрози

Першим кроком будь-якої атаки є розвідувальний етап, під час якого зловмисник збирає цінні розвідувальні дані про ціль. Він починається з проникнення на об'єкт (наприклад, у відкриті системи, пристрої) з метою вивчення можливих точок входу в систему. Далі, як показано на рисунку 1.4, противник майже завжди використовує різні методи для переліку розгорнутої інфраструктури. Інфільтрація ресурсів для індексації вразливих пристроїв Інтернету речей, розгорнутих у «розумних містах», зловмисник може здійснювати активне зондування в Інтернеті [29] або використовувати пошукову систему Shodan [30] для виявлення легких цілей з обліковими даними за замовчуванням [31]. Крім того, що сканування мережі є першим кроком будь-якої кібератаки, воно значно погіршує продуктивність мережі, сповільнюючи час відгуку на запити користувачів [32].

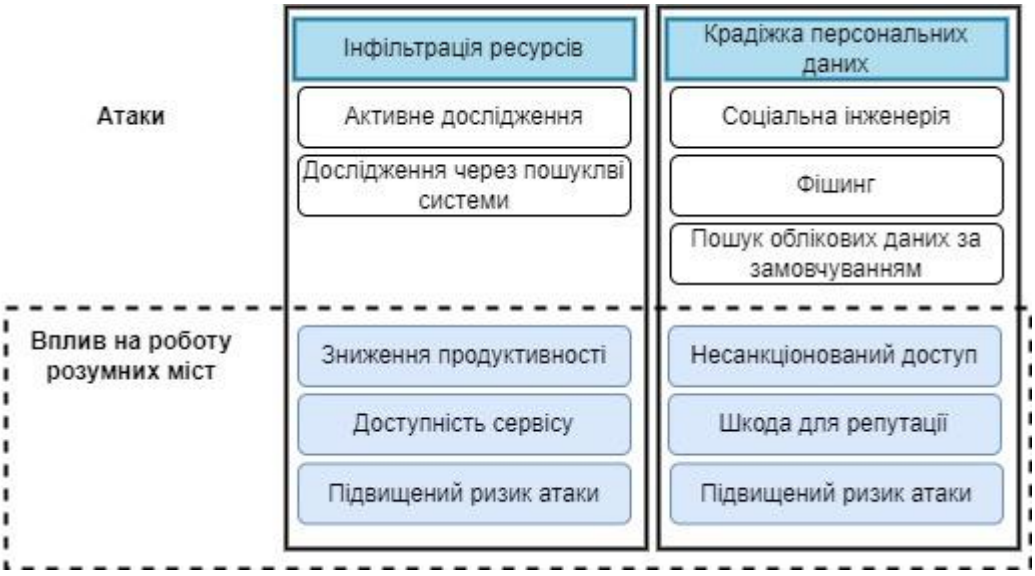

Рисунок 1.4 – Розвідувальні загрози в умовах розумних міст: атаки та наслідки

Крадіжка особистих даних передбачає отримання ідентифікаційних даних жертви для отримання привілейованого доступу до системи або даних, контролю над інфраструктурою та проведення різноманітних атак. Загроза має різні форми: облікові дані можуть бути вилучені з хешів, за допомогою соціальної інженерії та фішингу, а також шляхом використання слабких облікових даних пристроїв IoT. Останнє є особливою загрозою для розумних міст на основі Інтернету речей, оскільки їхні рішення покладаються на дані, зібрані датчиками Інтернету речей. Крім того, крадіжка облікових даних призводить до несанкціонованого доступу до ресурсів розумних міст. Дійсно, втрата контролю над інфраструктурою та даними підвищує ризик репутаційних збитків.

1.2.2 Диверсії інфраструктури

Однією з мотивацій зловмисників є отримання незаконного контролю над інфраструктурою шляхом втручання, маніпуляцій, перепрограмування або перевантаження ресурсів. На рисунку 1.5 показані атаки цієї категорії та їхній вплив на роботу «розумних міст».

Втручання в інфраструктуру Ця загроза може проявлятися двома способами: безпосередньо або віддалено. Оскільки велика кількість виконавчих

механізмів і датчиків працюють без нагляду, а політики і методології захисту від несанкціонованого втручання відсутні або обмежені, зловмисник може скористатися фізичним доступом до пристрою, щоб завдати йому значної шкоди, змінити його сервіси або отримати необмежений доступ до даних, що зберігаються в його пам'яті. Фактично, скомпрометовані приводи, які контролюють фізичну інфраструктуру (наприклад, опалення, комутаційні елементи тощо), можуть спровокувати пошкодження фізичних об'єктів і загрожувати громадській безпеці. Крім того, зловмисник може використати інфраструктуру розумних міст для залучення її до ботнету, спричиняючи як прямі, так і непрямі негативні наслідки. Перший полягає у втраті контролю над інфраструктурою та загрозі для критично важливих функцій міста. Опосередковано боти можуть бути використані зловмисником для проведення розподілених атак типу «відмова в обслуговуванні» (DDoS), збору інформації з мережі [33], майнінгу криптовалют [34], розповсюдження шкідливого програмного забезпечення [35], тощо. Насправді, непрямий вплив може призвести до погіршення продуктивності системи, на додаток до юридичної та комплаєнс-відповідальності. Більше того, зловмисник також може втрутитися в роботу пристрою, використовуючи вразливості прошивки [36].

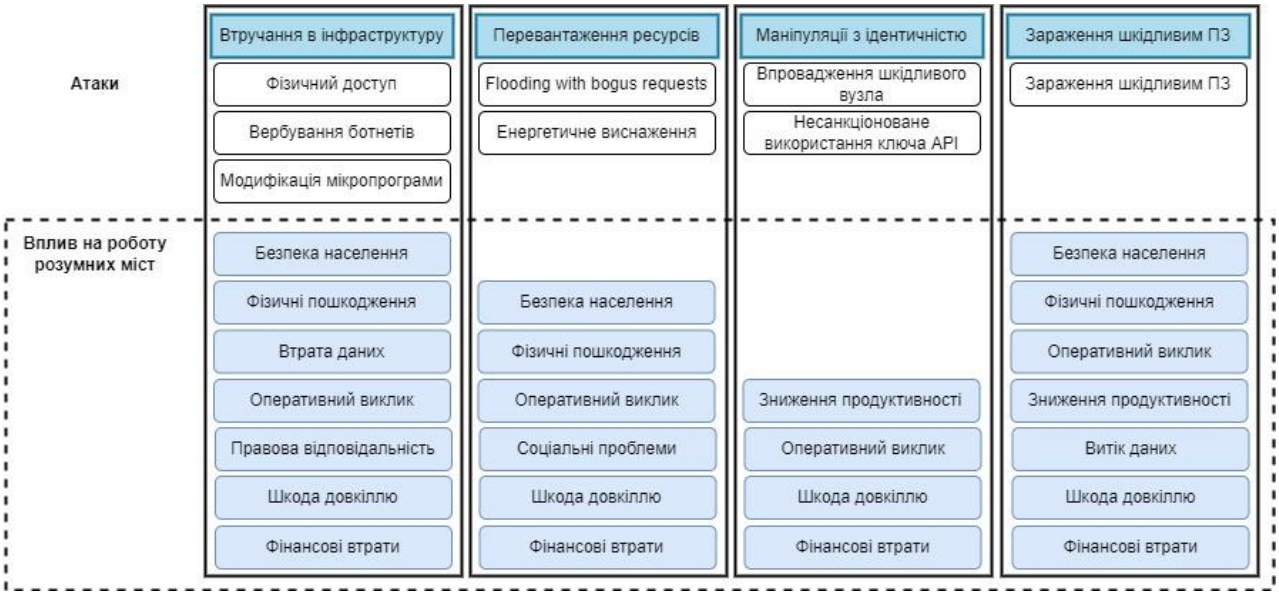

Рисунок 1.5 – Диверсії інфраструктури в умовах розумних міст: атаки та наслідки

Під час перенасичення ресурсами зловмисник намагається порушити роботу сервісу шляхом запобігання доступу до цього сервісу. Для цього він засипає ціль надмірною кількістю запитів. Як наслідок, сервіс не може обробити всі запити, а отже, законні користувачі не можуть отримати до нього доступ. Крім того, це загроза для API, оскільки сервіс не обмежує кількість отриманих запитів. Це також актуально для розумних міст на основі IoT, враховуючи обмежені обчислювальні можливості пристроїв IoT. Наприклад, у Фінляндії система управління будівлею була завалена фальшивими запитами, які змушували опалювальні прилади вимикатися [37]. Крім того, суворі правила безпеки та обмеження поширення радіохвиль не дозволяють вбудованим пристроям ефективно збирати енергію [38], що дозволяє зловмисникам викачувати енергію з інфраструктури "розумних" міст. Крім того, погані практики розробки програмного забезпечення можуть значно збільшити споживання енергії [39] і призвести до порушення роботи міста.

Маніпуляції з ідентифікаційними даними може виникати двома різними способами: або шляхом впровадження фальшивих датчиків, або шляхом використання несанкціонованих ключів API. Крім того, впровадження шкідливих вузлів у мережу призводить до погіршення продуктивності мережі.

Поширення шкідливого програмного забезпечення з метою зараження розумних датчиків, пристроїв IoT або серверів даних. З цією метою зловмисник намагається змінити їхні функції або здійснити витік конфіденційних даних. Наприклад, надсилання фальшивих повідомлень про перевантаження з великої кількості розумних лічильників може призвести до відключення кількох сегментів енергосистеми.

1.2.3 Маніпуляції з даними

Загрози маніпулювання даними проявляються чотирма різними способами: фальсифікація даних, пошкодження даних, нецільове використання та порушення процесу прийняття рішень. На Рисунку 1.6 показані атаки, пов'язані з цією категорією, та їхній вплив на роботу розумних міст.

Відомі випадки коли поширені атаки програм-вимагачів паралізували роботу багатьох «розумних міст». Вимагачі - це шкідливе програмне забезпечення, яке блокує обладнання або шифрує файли даних, поки не буде сплачено грошовий викуп, як правило, у криптовалюті. Через високий рівень взаємозв'язку в «розумних містах» цей тип загроз має значний вплив на їхню роботу. Наприклад, шкідливе програмне забезпечення SamSam взяло в заручники послуги, що надаються багатьма містами. Цей приклад показує, як підробка даних може саботувати функції, що залежать від даних, і призводить до масової втрати даних [9]. Крім того, якщо противник атакує життєво важливі сектори, такі як охорона здоров'я [40], неможливість доступу до даних пацієнтів може коштувати людських життів. Більше того, ми можемо кількісно оцінити атаки на дані в розумних містах, вимірявши їхні фінансові втрати. Наприклад, сплачений викуп, ціна відновлення даних і втрата роботи (наприклад, безкоштовних автобусних поїздок [41]) - ось кілька прикладів, які оцінюють фінансові втрати, спричинені такими атаками.

Незважаючи на те, що введення шкідливих даних в розумні давачі здається мінімальним [42], воно може спричинити драматичний економічний ефект або коштувати людських життів [43]. Наприклад, розумні лічильники можуть бути використані для крадіжки енергії у муніципалітетів [44]. Крім того, аварійні сповіщення можуть бути використані для створення хаосу [11]. Крім того, ці зловмисні дані можуть бути створені таким чином, що вони змушують моделі машинного навчання робити хибні прогнози і спричиняють нестабільність у роботі міста.

Нецільове використання даних несе за собою певні загрози. Інфраструктура «розумних міст» генерує величезні обсяги інформації. Ця інформація збирається з безлічі давачів і від громадян (коли це можливо, з їхнього дозволу). Крім того, зібрана інформація може бути використана для зловживання персональними даними з різних причин. Так, зловмисник може захотіти відстежити активність людини за допомогою датчиків або камер спостереження, прослухати комунікацію або скористатися слабким доступом до Інтернету, щоб викрасти облікові дані людини, які згодом можуть бути

використані для шахрайських транзакцій. Однак зловживання даними не обов'язково виникає тоді, коли зібрані дані використовуються в недозволених цілях [45].

Рисунок 1.6 – Загрози маніпуляції даними в умовах «розумних міст»: атаки та наслідки

Порушення процесу прийняття рішень: оскільки більшість «розумних міст» впроваджують алгоритми машинного навчання в якості механізму прийняття рішень, варто враховувати надійність таких алгоритмів. Фактично, зловмисники прагнуть порушити процес прийняття рішень шляхом отруєння даних або шляхом реалізації дослідницької атаки. У випадку зараження даних, механізм прийняття рішень компрометується шляхом введення ретельно розроблених зразків противника в навчальний набір даних з метою скомпрометувати процес навчання. Достовірність аналітики розумних міст буде продовжувати страждати, поки надійність таких алгоритмів не буде підтверджена. Це питання не менш актуальне і для надійності систем виявлення вторгнень, що базуються на алгоритмах машинного навчання [46]. У випадку дослідницьких атак противник намагається отримати інформацію, промацуючи систему, що навчається. Фактично, він діє шляхом введення зразків, які призначені для того, щоб обійти систему, що навчається, на етапі тестування з метою інверсії моделі або виведення інформації.

1.2.4 Сторонні вразливості

Адміністрація «розумних міст» зазвичай вирішує співпрацювати з приватним сектором, щоб подолати бюджетні та кваліфікаційні обмеження, одночасно сприяючи інноваціям та економічному розвитку. Фактично, приватний сектор розробляє і постачає відповідні технології, будує інфраструктуру, збирає і обробляє дані та розробляє програмне забезпечення для прийняття рішень. Однак ця стратегічна співпраця створює нові можливості для кіберзагроз. На Рисунку 1.7 показані такі загрози/вразливості, пов'язані з ними атаки та вплив цих атак на "розумні" міста.

Скомпрометований хмарний провайдер: хмарні обчислення відкривають нові можливості для розробників, пропонуючи інфраструктуру, платформи і програмне забезпечення через Інтернет. Дійсно, хмарні сервіси є привабливим варіантом для постійно зростаючих «розумних міст» завдяки низькому рівню початкових інвестицій, їх масштабованості та постійній доступності. Однак особливості хмарних обчислень, такі як багатокористувацьке використання та віртуалізація, можуть призвести до витоку приватної інформації та несанкціонованого доступу. Характерними прикладами таких атак є викрадення хмарних облікових записів та використання вразливостей системи [33].

Незахищені інтерфейси прикладного програмування (API) - це вразливість, яка відкриває двері до хмарних додатків та веб-сервісів. Фактично, API дозволяє користувачам налаштовувати свій досвід та отримувати доступ до багатьох веб-сервісів, включаючи автентифікацію та контроль доступу. Власне, API призначені для обміну інформацією. Тому вплив порушень API залежить від сервісу та інформації, що передається. Наприклад, у місті Лос-Анджелес відкритий текстовий ключ API дозволив хакеру скористатися платними сервісами Google [47].

Недбалий постачальник послуг: деякі постачальники впроваджують нові кібервразливості. Вони можуть навмисно або ненавмисно залишати бекдори, які дозволяють зловмисникам отримати доступ до пристроїв або програмного забезпечення. Вони можуть надалі розгортати пристрої Інтернету речей без

можливості виправлення. Хоча «розумні міста» часто використовують вразливі продукти без виправлень, деякі виробники не бажають визнавати наявність дірок у безпеці своїх продуктів, що ставить під загрозу операторів послуг "розумних" міст, а згодом і їхніх мешканців.

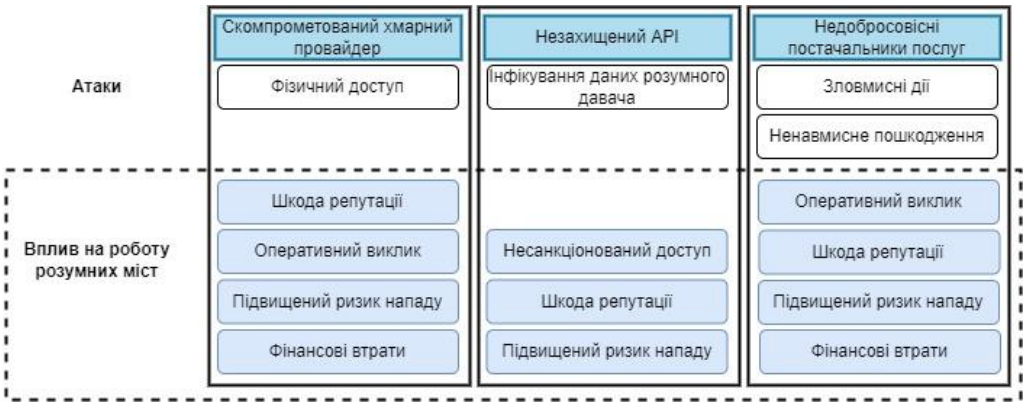

Рисунок 1.7 – Загрози сторонніх вразливостей в умовах «розумних міст»

1.3 Висновок до першого розділу

Крім того, з огляду на зростаючу кількість кібератак та їх вплив на безпеку мешканців міста і на застарілу інфраструктуру, а також відповідні фінансові проблеми, потрібні нові види ситуаційної обізнаності для подолання їх наслідків. У цьому сенсі відчутний брак комплексних досліджень методів підтримки кіберситуаційної обізнаності в контексті розумних міст. Насправді, поєднання модельованих залежностей окремих блоків «розумних міст» з дослідженням та синтезом контекстуалізованої розвідки загроз, методів оцінки ризиків та вразливостей, а також методів виявлення атак дозволить адаптивно моделювати загрози, враховуючи знання, отримані з різних джерел.

Архітектура «розумних міст» вразлива до традиційних комп'ютерних вірусів, віддалених зломів, підслуховування, викрадення програмного забезпечення, впровадження шкідливого вмісту та/або неправильно сформованих запитів, експлойтів пам'яті, доступу до конфіденційної інформації та неправомірного використання даних. Крім того, зв'язок з фізичним середовищем, впровадження пристроїв Інтернету речей та поява нових протоколів зв'язку, а також використання алгоритмів машинного навчання

створюють нові загрози безпеці та посилюють вплив традиційних вразливостей. Виходячи з вищезазначеної інформації, ми визначаємо наступні чотири класи загроз, як показано на рис. 3: дослідницькі загрози, саботаж інфраструктури, маніпуляції з даними та вразливості третіх сторін. Дійсно, величезна небезпека цих загроз корініться в підвищеній взаємозалежності між різними компонентами «розумних міст».

2 КАТЕГОРІЇ, МЕТОДИ ТА МОДЕЛІ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

Незважаючи на те, що описані загрози для «розумних міст» постійно еволюціонують, продовжує розроблятися багато передових методів для підтримки видимості кіберзагроз. У цьому розділі опишемо вибрані методи з подальшою їх категоризацією.

2.1 Моделі взаємозалежності

Різнорідні протоколи зв'язку та спільна інфраструктура з'єднують різні вбудовані системи, щоб зробити міста більш ефективними. Крім того, різні постачальники послуг обмінюються інформацією та ресурсами для підтримки сталого функціонування «розумного міста». Така висока взаємозалежність створює велику кількість можливих атак і вразливостей, які безпосередньо пов'язані з серйозністю загрози і мають мультиплікативний ефект на визначення пріоритетів пом'якшення наслідків. Дійсно, загроза, яка призводить до втрати одного сервісу або інфраструктури, може потенційно вплинути на інші сервіси, оскільки вони використовують ресурси один одного. Більше того, виявлення цих вразливостей та їхнього впливу є складним завданням через високу складність зв'язків між різними об'єктами інфраструктури. Крім того, кожен компонент «розумного міста» має різноманітні вимоги до безпеки, що створює додаткові виклики.

Будь-який збій у роботі систем «розумного міста» вплине на його ефективне функціонування, а також на безпеку та добробут його мешканців. Крім того, формальна модель взаємозв'язку елементів міста дозволить зрозуміти фундаментальні характеристики топології системи і може бути корисною при розробці профілю безпеки, оцінці сукупного впливу кіберзагроз та оцінці ефективності контрзаходів. Хоча розглянуті моделі залежностей не враховують кіберзагрози, розуміння зв'язку між різними доменами впливає на визначення пріоритетів загроз та їх пом'якшення.

З цією метою Лауге та ін. [48] продемонстрували, як збій в одній службі може вплинути на інші сфери. У цьому контексті дослідники провели серію інтерв'ю з експертами та кількісно оцінили величину негативного впливу на залежні послуги, такі як енергетика та зв'язок. Результати, які включають характеристику часового виміру для динамічного вивчення впливу, дозволили глибоко зрозуміти прямі та вищі залежності для визначення пріоритетів пом'якшення наслідків.

Крім того, Кьоніг та ін. [49] запропонували структуру для представлення впливу несприятливих подій у високозв'язних критичних інфраструктурах (КІ). Підхід моделює залежності між інфраструктурами у вигляді орієнтованого графа. Фактично, кожна КІ позначається як єдина вершина, а ребра символізують залежність від ресурсів інших КІ. Кожне ребро відноситься до класу $c \in \{1, 2, ...C\}$, який представляє фіксований тип внутрішньої або взаємної залежності. Крім того, ці залежності оцінюються за допомогою ланцюга Маркова та інтерв'ю з експертами. Крім того, візуалізація залежностей проілюструвала, як обмеження в одному КІ впливають на залежні КІ і як цей вплив змінюється з часом.

Щоб визначити мінімальну підмножину вузлів критичної інфраструктури та вибрати найбільш корисні пріоритети пом'якшення наслідків, Стергіопулос та ін. [50] ввели в свою модель граф ризиків залежностей і визначили кореляцію між метриками центральності та вузлами з високим впливом.

В іншій роботі Стергіопулос та ін. [51] змоделювали залежності між інфраструктурами у вигляді графа G= (N, E), де N - множина вершин, що представляють інфраструктури або компоненти, а E - множина ребер, які символізують залежності. Фактично, ребро від вузла CI_i до вузла CI_{ij}, тобто $CI_i \rightarrow CI_i$, позначає відношення ризику, яке є похідним від залежності інфраструктури CI_i від послуги, що надається інфраструктурою CI_i. Цей зв'язок кількісно оцінюється за допомогою впливу $I_{i,j}$ та ймовірності $L_{i,j}$ того, що збій буде реалізовано. Крім того, каскадний результуючий ризик представлений як числове значення кожного ребра. Потім рівень зростання попередньо обчислюється і передається до нечіткої системи ранжування, яка забезпечує реалістичну оцінку еволюції потенційних збоїв.

Однією з цілей роботи Беккуті та ін. [52] було дослідити наслідки несправної системи зв'язку, коли в електромережі стався збій. З цією метою автори змоделювали та імітували електричний стан електроенергетичної системи (EEC) за допомогою стохастичної мережі активності (SAN). На противагу цьому, атака на відмову в обслуговуванні (DoS) була змодельована за допомогою стохастичних добре сформованих мереж (SWN). В іншій роботі Блумфілд та ін. [53] зосередили своє дослідження на тому, як сила залежностей між енергетичними та телекомунікаційними мережами впливає на різні показники ризику та невизначеності.

Науковці в [54] використовували стохастичне моделювання промислової системи управління і вивчали вплив як випадкових збоїв, так і кібератак. Фактично, дослідники використовували стохастичний автомат для моделювання поведінки супротивника, тоді як залежності між елементами моделювалися з використанням детермінованого або імовірнісного підходу. Вивчення застосованого підходу дозволило виявити найбільш критичні елементи мережі та високу кореляцію між впливом і можливостями зловмисників. Далі Йохансен та ін. [55] запропонували моделювати взаємозалежності за допомогою байєсівської мережі та формулювання мінімальної множини зв'язків (MLS) для створення мережевої моделі. Крім того, в роботі [56] запропонували метод моделювання залежностей, який підтримує дослідження каскадного ефекту, виконує аналіз вразливостей та планує стратегії обслуговування. Автори продемонстрували, як відкритий гібридний автомат дозволяє моделювати окремі підсистеми та компонувати їх разом для створення більш складних та детальних систем з метою врахування різних типів залежностей. В іншій роботі [57] проаналізували проблему розподілу ресурсів безпеки між різними компонентами взаємозалежних кіберфізичних систем (КФС) з метою захисту всієї екосистеми від кібератак.

2.2 Оцінка ризиків та розвідка загроз

Зростаюча кількість і масштаби кіберзагроз вимагають проактивних рішень для розвитку широких можливостей кібербезпеки. Насправді, основними викликами для прийняття рішень у сфері кібербезпеки є невизначеність кіберзагроз та їхньої серйозності, а також технологічний прогрес, який створює нові вразливості. Враховуючи неоднорідність пристроїв Інтернету речей, безліч вразливостей потребують виправлення та моніторингу. Тому вкрай важливо визначити пріоритетність захисту критичних вразливостей та ефективно розподілити час і бюджет. Контекстуалізовані можливості розвідки кіберзагроз доповнюють завдання оцінки ризиків, допомагаючи виявляти невідомі інциденти, тенденції атак, оцінюючи і розуміючи їх наслідки.

У контексті оцінки ризиків Лі та ін. [58] оцінили ризик кібербезпеки в системах світлофорів. Спочатку автори застосували теоретико-ігрову базу для визначення найгіршої ефективності управління дорожнім рухом під час атаки. Потім ця метрика використовується для визначення серйозності конкретної атаки як $S_i = P_0 - P_i^*$, де P_0 представляє продуктивність системи, яка не піддається атаці, а P_i^* - продуктивність системи під час атаки. Потім дослідники визначили ризик кібербезпеки системи світлофорів за певних умов дорожньої мережі, розрахувавши його як $R = \sum_{i \in C} L_i * S_i$. Далі було сформульовано систему зменшення кібер-ризиків з використанням суб'єктивного правила прийняття рішень, відомого як критерій мінімаксного жалю. Тут жаль визначається як ризик за певних умов трафіку без застосування контрзаходів. Крім того, ранжовані контрзаходи дозволяють мінімізувати найгірший випадок жалю.

Келарестагі та ін. [59] провели оцінку ризику, орієнтовану на вразливість, використовуючи модель ризику Національного інституту стандартів і технологій (NIST). Автори синтезували реальні правопорушення та наукові публікації, які вивчають атаки на вразливості бортових мереж, щоб кількісно оцінити потенційний вплив експлуатації. В іншій роботі науковці [60] оцінили можливий каскадний вплив одного інциденту на декілька КІ. По суті, цей підхід моделює

зв'язки між об'єктами інфраструктури у вигляді графа, ребра якого представляють залежності в умовах звичайної експлуатації. Крім того, метод не диференціює ризики, а використовує вплив несприятливих наслідків як результат оцінки ризиків для кожної інфраструктури.

Важко переоцінити важливість Інтернету речей в екосистемі «розумного міста». З огляду на різноманітність пристроїв IoT, вразливості всієї системи незліченні [61]. Сікарі та ін. [62] запропонували методологію оцінки ризиків загального призначення в контексті розгортання IoT. Спочатку вони визначають компоненти моделі та формують дерево атак, вузли якого представляють різні способи атак, а листя символізують вразливості v_i. Дійсно, кожна вразливість пов'язана з рівнем вразливості E_i. Останній вказує на міру того, наскільки ймовірно, що вразливість v_i буде використана для здійснення атаки. На наступному кроці фреймворк моделює граф, який відображає залежності d_i між v_i. Потім кожному ребру графа присвоюється рівень вразливості, який оновлюється за формулою

$$E_{i+1} = \max\left(E_0(v_i), \min\left(E(d_i), E_i(E_i)\right)\right) \qquad (2.1)$$

Вираз 2.1 вказує на ризик експлуатації. Крім того, цей підхід забезпечує масштабованість з точки зору легкого додавання або видалення компонентів з фреймворку.

Крім того, Ван та ін. [63] запропонували метод оцінки вразливостей, заснований на атрибутивному графі атак. [64]. Vодель використовує алгоритм розширеного шляху, щоб запропонувати порядок пріоритетності атак і визначити найслабшу ланку в системі, щоб визначити пріоритетність їх моніторингу та захисту.

У додатковій роботі Раданлієв та ін. [65] запропонували систему оцінки економічних наслідків для IoT. Автори використали модель Cyber Value at Risk для вимірювання максимально можливих втрат за певний період часу та модель MicroMort для прогнозування невизначеності за допомогою одиниць ризику смертності. Назіруддін [66] використав процес прийняття рішень Маркова для

моделювання безпеки розумних міст на високому рівні абстракції. Модель враховує компоненти системи та їх типи (наприклад, датчик, привід тощо), кібератаки на кожен елемент, вразливості з ймовірностями експлуатації, які витягуються з бази даних CVSS, та людське втручання на останньому рівні захисту.

Шиврадж та ін. [67] запропонували загальну систему оцінки ризиків для систем IoT. Автори описали інформаційний потік через різні компоненти як зважений спрямований ациклічний граф G(V, E) . Ребро E між вузлами V вказує на залежність одного вузла від іншого. Дійсно, один вузол може бути з'єднаний з кількома іншими, утворюючи численні зв'язки.

Мохсін та ін. [68] запропонували імовірнісну модель для автоматичної оцінки ймовірності реалізації загрози в різних конфігураціях систем IoT. На першому етапі фреймворк використовує модель Маркова для представлення архітектури системи, загроз безпеці та можливостей зловмисників, щоб спрогнозувати ймовірність атаки та запропонувати безпечну конфігурацію.

Однією з основних цілей розширеного виявлення загроз є визначення потенційного прогресу виявленої шкідливої події в екосистемі. У цьому контексті Фалько та ін. [69] розробили метод автоматичної ідентифікації стратегій атак, які можуть бути використані для компрометації мережі відеоспостереження. Підхід поєднує в собі кілька встановлених фреймворків для розгляду повного життєвого циклу атаки. Анджеліні та ін. [70] пов'язали топологію та географію мережі з результуючим впливом, використовуючи візуалізацію, засновану на сферах корупції. Цей метод був використаний для того, щоб сконцентрувати увагу на найбільш шкідливому ризику кіберінцидентів.

Щоб проаналізувати ступінь експлуатації, Ван та ін. [71] виміряли фактори загроз для розумних міст, об'єднавши понад 200 зібраних характеристик на основі підходу «Апаратне забезпечення, інтелект, програмне забезпечення, політика та експлуатація» (HiSPO) [72]. Після присвоєння ваги $w_i = 1/\sum_i(r_i)$ кожній загрозі, фактор загрози розраховувався як

$$t = 0.5 * \sum w_i * (t_i + \delta) + 0.001 * (C_B + C_T + C_E) + 0.02 * f_{TI} \quad (2.2)$$

Де C_B, C_T, C_E - базова, тимчасова та екологічна оцінки в CVSS відповідно. Крім того, скоригована вага загрози позначається як δ , тоді як fTI символізує значення інтелектуалізації загрози. Крім того, у фінальному звіті представлені коефіцієнти загроз, які були розраховані до пом'якшення наслідків і після періоду оцінки та пом'якшення наслідків. Крім того, він показав, що запропонована методологія може значно мінімізувати ризики для розумних міст.

В іншій роботі Бу-Харб та ін. [73] створили прототип платформи розвідки кіберзагроз IoT для виявлення та розкриття скомпрометованих пристроїв IoT в масштабах Інтернету. З цією метою автори об'єднали результати пасивних і активних вимірювань аналізу мережевого трафіку в Інтернеті.

Крім того, «медові горщики» заманюють зловмисника в пастку, навмисно створюючи вразливості в певних технологіях. Ці пристрої (або програмне забезпечення) записують шкідливі дії, щоб надалі дослідити вектори і моделі атак. З огляду на те, що пристрої Інтернету речей на базі ZigBee активно використовуються в середовищах розумних міст [74], honeypot, що імітує шлюз ZigBee, запропонований Даулінгом та ін. [75], є корисним для дослідження атак на «розумні міста». Після 3-місячного моніторингу активності, спрямованої на шлюз ZigBee, дослідники повідомили про 6 типів виконаних атак. До них відносяться словникові атаки і атаки грубої сили, сканування, ботнети і ряд інших незалежних подій. Автори також повідомили, що на атаки по словнику припадає майже 94% всіх атак.

2.3 Методи виявлення атак

Оцінка загроз на основі даних, хоч і є надзвичайно цінною та глибокою, не може охопити всі можливі можливості загроз. З цією метою ретроспективний аналіз інцидентів фіксує кілька атрибутів загроз і системних характеристик, що дозволяє виміряти ефективність впроваджених механізмів захисту. Дійсно, наукові зусилля, спрямовані на розробку переконливих методів виявлення загроз

і зловмисних подій, вивчалися протягом десятиліть, що призвело до появи безлічі методів виведення. Останнім часом спостерігається тенденція до використання методів машинного навчання, які вирішують проблему розпізнавання зловмисних шаблонів у (мережевих) потоках даних/трафіку з метою виявлення аномалій.

У цьому ключі основною метою роботи, проведеної Оза та ін. [76], є виявлення атак повторного відтворення - підмножини атак введення неправдивих даних - у спробі захистити світлофори. Дійсно, такі атаки мінімізують ефективність систем управління дорожнім рухом і потенційно можуть створювати небезпечні для життя ситуації. Для виявлення крадіжок енергії Хе та ін. [77] спробували виявити потенційні зловмисні ін'єкції в контексті електромережі. Автори запропонували схему в режимі реального часу для фіксації поведінкових особливостей атак на фальшиві ін'єкції даних.

Інфраструктура «розумних міст», особливо ті аспекти, що стосуються пристроїв Інтернету речей, може бути заражена шкідливим програмним забезпеченням або залучена до бот-мереж для проведення DDoS-атак та інших скоординованих заходів. З цією метою Азмудех та ін. [78] застосували мережу згортки до векторного представлення операційних кодів (OpCodes) для виявлення шкідливого програмного забезпечення IoT. Модель спочатку генерує граф операційних кодів, а потім перетворює його у власний простір (тобто у власний вектор і власне значення), щоб передати його на вхід згорткової мережі.

Далі Довом та ін. [79] запропонували метод класифікації шкідливих програм, заснований на нечітких і швидких нечітких деревах образів, які були застосовані до векторного представлення послідовностей операційних кодів. У двох словах, нечіткий класифікатор шаблонів - це набір нечітких дерев шаблонів $PT = \{PTi | i = 1, \dots k\}$ де кожне PTi - це дерево образів, пов'язане з класом $y_i \in \{malware, begin\}$, доброякісне. Дерево, яке дає вищу оцінку $\hat{y} = argmax(PT_i(x))f\ y_i\ or\ \in \{malware, begin\}$, потім використовується для присвоєння класу. Насправді, автори використали виграш в інформативності для класів, щоб вибрати найбільш корисні ознаки для генерації графа потоків. Крім того, запропонований метод перевершив класифікатори SVM, KNN,

випадкового лісу та дерева рішень. Крім того, запропонований метод продемонстрував загальний потенціал у взаємодії з шумом і невизначеністю, що робить його важливим рішенням для розгортання на периферії мережі.

Зловмисна поведінка завербованих пристроїв Інтернету речей (у ботнетах) може бути виявлена на різних етапах атаки. У цьому напрямку Кумар та ін. [80] намагалися виявити окремих ботів до фактичної атаки, тобто на етапі сканування. Вони проаналізували мережеву активність для раннього виявлення окремих ботів. Для цього було використано кілька алгоритмів машинного навчання, таких як Random Forest, KNN та Gaussian Naive Bayes, для маркування мережевого трафіку, який демонструє поведінку, схожу на поведінку IoT-ботнетів. Щоб підвищити продуктивність методу, автори оперували з агрегованим трафіком, щоб виявити рівень шлюзу доступу до Інтернету речей. Цей метод виявився швидшим і зменшив необхідний обсяг пам'яті.

З іншого боку, оскільки деякі зловмисники робили успішні спроби уникнути виявлення, дуже важливо мати можливість виявляти інфекції на більш пізніх стадіях атаки. З цією метою Мейдан та ін. [81] запропонували N-BaIoT, мережевий підхід, який виявляє скомпрометовані пристрої IoT, що використовуються для запуску атак. Підхід витягує статистичні характеристики, які фіксують поведінку мережі, і використовує глибокі автокодери (DAE) для виявлення аномального мережевого трафіку, що генерується скомпрометованими пристроями IoT. Було доведено, що цей метод здатний виявляти раніше небачені ботнети з низьким рівнем помилкових тривог, що має вирішальне значення для розподілу ресурсів.

В альтернативній роботі Алазаб та ін. [82] запропонували метод виявлення, який семантично дискримінує ботнети і перевіряє поведінкову легітимність численних додатків на основі Раза та ін. [83] запропонували метод виявлення атак всередині мережевого протоколу 6LoWPAN, який активно використовується в рішеннях для розумного освітлення. У розширеній версії [84] автори використовували метрики очікуваних передач (ETX), які вимірюються шляхом надсилання періодичних пробних пакетів між сусідами-учасниками.

Моделюючи нелінійну кореляцію між кількома часовими рядами, Лі та ін. [85] розробили некерований метод виявлення аномалій на основі GAN (GAN-AD) для виявлення атак в багатопроцесорних CPS з різними мережевими датчиками і виконавчими пристроями. Крім того, для виявлення криптографічних програм-вимагачів у мережах IoT Azmoodeh та ін. [86] класифікували патерни використання енергії на вузлах IoT та дискримінували вузли, інфіковані програмами-вимагачами. На першому етапі методологія фіксувала послідовність використання енергії для кожного процесу цільових пристроїв, після чого розраховувалася відстань, яка вимірює оптимальне вирівнювання між двома залежними від часу послідовностями, відомими як динамічне викривлення часу (Dynamic Time Warping, DTW). Нарешті, автори застосували три класифікатори, а саме нейронну мережу, SVM і KNN. У поєднанні з динамічним викривленням часу KNN перевершив інші класифікатори і продемонстрував чудову ефективність (94,27%) у виявленні програм-вимагачів у вузлах IoT.

Одна з найбільших проблем кібербезпеки безпосередньо пов'язана з нездатністю методів машинного навчання боротися з ворожими атаками. Дійсно, проактивні методи захисту на основі даних, спрямовані на боротьбу з атаками на алгоритми машинного навчання, пропонують дезінфікувати навчальні та тестові дані шляхом виявлення шкідливих ін'єкцій. Наприклад, Баракальдо та ін. [87] використовували дані про походження, які складаються з метаданих, що описують походження і родовід кожної точки даних, для виявлення зловмисних маніпуляцій з навчальними даними. Крім того, фреймворк, запропонований науковцями в роботі [88], кластеризує простір ознак вхідних даних і відфільтровує підозрілі точки даних. Метод обчислює середню відстань кожної точки даних від інших точок у тому ж кластері. Потім він розглядає мітку класу як додаткову ознаку з відповідною вагою. Крім того, точки даних з рівнем довіри менше 95% видаляються з навчальних даних для досягнення чистоти вхідних даних. Більше того, емпіричні експерименти продемонстрували значне покращення точності SVM-класифікатора.

2.4 Теоретичне підґрунтя

Доцільно виділити два класи моделей на основі їх теоретичного підґрунтя, а саме: машинне навчання та інтелектуальний аналіз даних, та другий: моделі, що базуються на знаннях. Перший клас складається з методів, які виводять складні можливості зіставлення шаблонів з навчальними даними; отже, він включає в себе етап навчання. Другий клас складається з методів, які вимагають створення бази знань, що відображає систему або профіль безпеки. Ці класи разом з їхніми підкласами показано на рис. 2.1.

Рисунок 2.1 – Класи моделей на основі теоретичного підгрунтя

2.4.1 Машинне навчання та методи аналізу даних

Глибокий автокодер (Deep autoencoder, DAE) - це багатошарова нейронна мережа прямого поширення, яка навчена стискати та реконструювати вхідні дані з мінімальною різницею між входом та виходом [89]. $\bar{X} = D(E(X))$ де X і $\bar{X}$ - вхід і вихід, відповідно, E - кодер від входу до прихованого шару, а D - декодер від прихованого шару до виходу. Дійсно, DAE призначений для визначення пріоритетності властивостей X, які повинні бути скопійовані в $\bar{X}$. Таким чином, він вивчає важливі властивості вихідних даних. Крім того, мету DAE можна формалізувати як наступну оптимізаційну задачу: $min_{D,E} \parallel -D(E(X)) \parallel$.

Мережі глибокого переконання (Deep Belief Networks, DBN) [90] складаються з декількох шарів стохастичних і латентних змінних і можуть розглядатися як особлива форма байєсівської імовірнісної генеративної моделі.

Згорткова мережа - це нейронна мережа, яка складається зі згорткового шару та шару субдискретизації, за яким слідують повністю з'єднані шари. Фактично, згортковий шар має k ядер, які діють як детектор ознак.

Дерево нечітких образів [91] - деревоподібна структура, в якій внутрішні вузли є арифметичними операторами нечіткої логіки, а вузли листя асоціюються з нечіткими предикатами вхідних атрибутів.

Генеративні змагальні мережі (Generative Adversarial Networks, GANs) [92] - це генеративно-дискримінативна архітектура глибокого навчання, яка складається з двох конкуруючих моделей нейронних мереж, а саме генератора (G) і дискримінатора (D). На першому кроці генератор отримує шум z для вивчення розподілу p_z . На основі сприйнятого розподілу генератор G формує вибірки даних і передає їх дискримінатору D . Потім дискримінатор використовує дивергенцію Дженсена-Шеннона для визначення розподілу між справжніми та фальшивими даними і передає ймовірність автентичності даних генератору G . Крім того, генератор згодом адаптує свої параметри на основі отриманої інформації про градієнт і передає нові зразки до D . Цілі генератора та дискримінатора можна формалізувати у вигляді наступної мінімаксної гри з функцією цінності:

$$V(D,G): min_G\, max_D\, V(D,G)$$
$$= \mathbb{E}_{x\sim p_{data}(x)}[log\ (D(x))] + \mathbb{E}_{z\sim p_z(z)}[log\ (1\ -\ D(G(z))] \qquad (2.3)$$

де p_{data} - розподіл даних, а p_z - попередній розподіл генеративної мережі.

Наївний баєсів класифікатор - це байєсівська мережа з одним кореневим вузлом, який представляє клас, і n листовими вузлами, які представляють атрибути. Наївний класифікатор Байєса визначається як n $N(a) = argmax_{c\in C}\, P(c)\, \prod_{i=1}^{n} P(xi|c)$, де $a = \{X1 = x1, \ldots, Xn = xn\}$ є повною множиною У даному методі кожна ознака визначається гауссівською функцією

густини ймовірності (PDF) як $X_i \sim N(\mu, \sigma^2)(x) = \frac{1}{\sqrt{2\pi\sigma^2}}$, де μ - середнє значення, а σ^2- дисперсія.

Класифікатор випадкових лісів - це метод машинного навчання, який використовує дерева рішень та ансамблеве навчання. Дійсно, ліси - це набір деревовидних класифікаторів , $\{h(x, \Theta_k), k = 1, \ldots\}$, де $\{\Theta_k\}$ незалежні однаково розподілені випадкові вектори, і кожному дереву присвоюється голос за найпопулярніший клас на вході x. Фактично, передбачення може бути зроблено на основі голосування більшості або зваженого голосування. Крім того, випадкові ліси можуть використовувати велику кількість атрибутів і тому не потребують відбору ознак. Ще однією перевагою цього класифікатора є його стійкість до перенавчання. Однак він сильно залежить від реалізованого генератора випадкових чисел і має недоліки в інтерпретації моделі.

k-найближчих сусідів - популярний метод машинного навчання, який не має фази навчання, а натомість запам'ятовує навчальні дані. Дійсно, щоб передбачити клас невидимого екземпляра, класифікатор KNN вимірює схожість між точками даних за допомогою евклідової відстані $d(x, y) = \sqrt{\sum_{k=1}^{n}(x_k - y_k)^2}$, де x_k, y_k - це елементи, що характеризують екземпляри x та y, відповідно.

2.4.2 Моделі на основі знань

Теорія графів У контексті кібербезпеки графи можуть описувати передумови атаки (вразливості) або шляхи атаки. Алгоритм пошуку найкоротшого шляху в дереві визначає індекс вразливості системи або оптимальний маршрут атаки з точки зору зловмисника. Фактично, доповнення наведених вище графів контрзаходами сприяє визначенню пріоритетів захисту.

Теорія ігор - це математичне моделювання взаємодії між агентами. Формальна теорія визначає гру як $Game = (Pi, S, s, \pi i)$, де P_i позначає гравців (i = 1, 2, ...), S - множина чистих стратегій для кожного гравця I, s : $S_1 \times S_2$ - множина профілів чистих стратегій, а πi : S → R - функції виграшів гравців. Далі

розв'язок гри представляється як оптимальні рішення гравців, які можуть мати взаємні або конфліктуючі інтереси.

Марковський процес прийняття рішень (MDP) - це стохастичний процес, який визначається як кортеж (S, A, P_a, R_a), де S - скінченна множина станів, A - скінченна множина дій, Pa - ймовірність того, що дія a в стані s в момент часу t призведе до стану s′ в момент часу t+1, а R_a - винагорода, яку очікується отримати після переходу зі стану s в s′ внаслідок дії a . Більше того, результатом MDP є політика π, яка ставить у відповідність кожному стану дію a, здійснену в цьому стані s. Крім того, процес має важливу властивість: дія залежить лише від поточного стану, а не від попередньої історії. Крім того, політика може бути реалізована через таблицю пошуку, або може включати великі обчислення [93].

Машина стану - це абстрактна модель, яка показує, як вихід обчислюється на основі вхідних даних. Математично модель формулюється як $SM = (\Sigma, S, s_0, \delta, F)$, де Σ - скінченна множина символів, S - скінченна множина станів, s_0 - початковий стан S, δ - функція переходу стану δ : S × Σ → S і F - скінченна множина кінцевих станів.

Стохастичні мережі активності (англ. Stochastic Activity Networks, SAN) [94] використовуються для оцінювання продуктивності, надійності та працездатності. Як стохастичне розширення мереж Петрі, SAN складається з наступних елементів: місць, воріт і робіт. Дійсно, ворота з'єднують місця з роботами (вхідні ворота) і роботи з місцями (вихідні ворота). Крім того, роботи можуть бути миттєвими та часовими, тобто такими, що мають затримку до завершення. Крім того, формально $SAN = ((P, A, I, O, \gamma, \tau, \iota, o), \mu_0, C, F, G)$, де P - скінченна множина місць, A - скінченна множина робіт, I - скінченна множина вхідних воріт, O - скінченна множина вихідних воріт, γ - кількість випадків для кожної роботи, τ задає тип роботи, ι зіставляє вхідні воріт з роботами і o зіставляє вихідні воріт з місцями.

Стохастичні добре сформовані мережі (англ. Stochastic Well-formed Nets, SWN) [95] - це системна модель, яка відображає основні характеристики складних систем з великою кількістю взаємопов'язаних компонентів.

Математично вона визначається як SWN = (WN, θ), де WN - добре сформована кольорова мережа Петрі, а θ - функція переходів.

Теорія конкуруючих ризиків [96] оцінює конкретний ризик в умовах складної присутності інших k ризиків і намагається передбачити наслідки усунення цього ризику.

Моделювання методом Монте-Карло - це математичний метод генерування випадкових величин для моделювання ризику або невизначеності певної системи.

2.5 Візуальний супровід

Не менш важливо, що кібербезпека, яка ґрунтується на аналітиці, повинна пропонувати візуальну підтримку, щоб залучити людське пізнання для інтерпретації даних. Візуальна аналітика поєднує обчислювальні методи аналізу даних і людські міркування в процесі прийняття рішень за допомогою візуалізації та взаємодії. Дійсно, графічне представлення надає широкий спектр візуальних засобів для розуміння того, як працює модель, для представлення результатів в інтуїтивно зрозумілій формі, а також для забезпечення взаємодії для візуального дослідження даних. Хоча розглянуті роботи не були присвячені створенню наочних посібників, ми порівнюємо візуальні виміри, щоб зрозуміти роль візуалізації в аналітичному аналізі. Для цього можна виділити три категорії, а саме: візуалізація ефективності, пояснення моделі та вилучення знань.

1. Візуалізація ефективності - це графічне представлення точності моделі, в тому числі точності, досягнутої за допомогою різних параметрів моделі.

2. Пояснення моделі - це процес інтерпретації виявлених знань у вигляді візуальної графіки. Перше, що тут слід розглянути, - це візуалізація архітектури моделі, зокрема, як розроблена модель і потік даних. Крім того, обчислювальні графіки та блок-схеми в достатній мірі відображають архітектуру. Крім того, іншими компонентами для візуалізації є параметри моделі, внесок різних вхідних даних (тобто ознак) та вимірювання помилок (наприклад, ті, що генеруються зразками змагальної мережі на кожному кроці).

3. Видобування знань використовує людські знання, що дозволяє користувачам більш ефективно інтерпретувати дані і формулювати гіпотези. Насправді, методи взаємодії, такі як деталізація на вимогу, динамічні запити та масштабування, можуть значно покращити цей процес.

Незважаючи на те, що близько 50% робіт все ще не використовують метод візуалізації, дослідники знайшли спосіб візуально прояснити модель як засіб пояснення методу. Дійсно, діаграми розсіювання, лінійні та гістограми поступово використовуються як візуальна структура для пояснення моделі. Фактично, більшість дослідників використовували просторове уявлення у вигляді 2-вимірного представлення даних, тоді як поєднання фізичної та 2-вимірної структури використано лише в одній роботі. Крім того, менше 40% досліджених моделей підтримують візуалізацію результатів. Серед них лише одна робота пропонує інтерактивність, тоді як решта робіт покладаються виключно на неінтерактивні представлення.

Хоча автоматизовані алгоритми роблять можливим розпізнавання образів, класифікацію та інші функції, поєднання цих алгоритмів з візуальною аналітикою, безсумнівно, може покращити процес прийняття рішень.

2.6 Вихідні дані: введення, інтерпретація та набори даних

Розглянуті роботи створили основу для дослідників, отримавши базові дані двома способами: використовуючи існуючі набори даних і збираючи дані шляхом створення специфічних умов у лабораторних умовах. Перші методи є досить ефективними, оскільки дозволяють уникнути будь-якого збору даних. Однак спостерігається дефіцит наборів даних, пов'язаних з «розумними містами». Тому другий метод збору даних є дуже продуманим. Тим не менш, він, як правило, підходить лише для короткострокового збору, його важко відтворити, і він ледве охоплює всю інфраструктуру розумних міст.

З огляду на відсутність публічних наборів даних, створених для «розумних міст», загальні приклади і кілька наборів даних були отримані в лабораторних умовах. Однак такі налаштування не відображають контекст

«розумних міст». Тому вони рідко ґрунтуються на реалістичних припущеннях, а отже, їх практична реалізація не завжди може бути успішною або репрезентативною.

Тому застосуємо короткий опис використаних публічних наборів даних. Набір даних SWaT 2016 року [98] підтримує дослідження в галузі розробки безпечних кіберфізичних систем (КФС). Дійсно, збір даних проводився на шестиступеневому тестовому стенді безпечної обробки води (SWaT), який являє собою зменшену версію промислової водоочисної станції. Крім того, набір даних складається з двох поведінкових моделей, зібраних під час нормальної роботи та під час атаки на систему. Більше того, фізичні властивості даних разом з мережевим трафіком містять атаки, здійснені дослідниками, і надають точні мітки даних для подальшого використання.

Shodan [99] - це пошукова система для пристроїв, підключених до Інтернету. Вона сканує Інтернет 24/7 і оновлює свій репозиторій в режимі реального часу, щоб надати найсвіжіший список пристроїв Інтернету речей. Крім того, перехоплюючи та аналізуючи банери та метадані пристроїв, система досліджує відповідні вразливості (включаючи Heartbleed, Logjam та паролі за замовчуванням).

IoT Scanner від BullGuard - це онлайн-пошукова система, яка використовує сервіс Shodan, щоб дозволити користувачам сканувати свої мережі на наявність вразливостей.

Даркнет [100] (також відомий як мережевий телескоп) - це набір маршрутизованих і розподілених, але невикористаних IP-адрес. З точки зору дизайну, даркнет є прозорим і невидимим у порівнянні з рештою інтернет-простору. З точки зору розгортання, вона забезпечується мережевими датчиками, які впроваджуються і розосереджуються в численних стратегічних точках по всьому Інтернету. Мета даркнету - відстежувати небажаний трафік в Інтернеті; оскільки IP-адреси даркнету не використовуються, будь-який трафік, спрямований на них, є аномальним трафіком.

Всі зразки програм-вимагачів і шкідливих програм збираються за допомогою VirusTotal. Дійсно, цей сервіс об'єднує результати роботи різних

антивірусних програм і онлайн-сканерів, щоб перевірити, чи вказує поведінка програмного забезпечення на зловмисну діяльність, чи ні.

Крім того, за допомогою публічного API користувачі можуть автоматично завантажувати та перевіряти свої файли.

2.7 Показники порівняння та оцінки моделей

2.7.1 Моделі взаємозалежності

Для порівняння методів та моделей взаємозалежності, розглянемо такі критерії: категорії залежностей, повнота та підхід до моделювання.

Категорії залежностей: це критерій, що стосується типів взаємозалежностей, які моделює кожен метод. У цьому контексті класифікуємо їх як кібернетичні, фізичні та функціональні залежності [101]. Крім того, називаємо модельовані залежності кібернетичними, якщо стан однієї області залежить від інформації, що передається іншою. Крім того, фізичні залежності представляють мережі, які мають спільний фізичний потік. Крім того, функціональні залежності враховують вплив деградації однієї сфери (або її наявності) на продуктивність залежної інфраструктури.

Масштаб – це критерій, що вимірює охоплення розглянутих методів. Очевидно, що кількість розглянутих залежних доменів безпосередньо впливає на повноту модельованої архітектури.

Підхід до моделювання - це критерій визначає метод на основі методу, який використовується для моделювання залежностей: імовірнісний (P), метод експертних оцінок (E) або детермінований (D).

2.7.2 Методи оцінки ризиків

Однією з найбільш значущих проблем методів визначення пріоритетів в «розумному місті» є оцінка запропонованого підходу. Ця проблема підтверджується відсутністю стандартних метрик оцінки в розглянутих роботах.

Оскільки вибір методології оцінки ризиків залежить від інфраструктури системи, вимог безпеки та мети [102], ми визначаємо наступний набір метрик для оцінки достатності кожної моделі.

Перспективність – це критерій, який фокусується на рівні ресурсів, що використовуються для ідентифікації ризику. Він може бути описаний як три категорії: метод, керований активами, метод, керований послугами, і метод, керований бізнесом [102].

Сфера застосування – це переплетена архітектура розумних міст робить оцінку впливу набагато складнішою, ніж у традиційних ІКТ-середовищах. Дійсно, така інфраструктура складається з безлічі різнорідних пристроїв, комунікаційних протоколів і екосистем великих даних, не кажучи вже про тісний взаємозв'язок між елементами архітектури. iii. Сфера кібербезпеки Зазвичай під сферою кібербезпеки розуміють вплив на основні цілі кібербезпеки, а саме: конфіденційність, цілісність, доступність та підзвітність.

Стратегія ідентифікації загроз передбачає наступне, а саме два основні підходи: ручний та автоматичний. Останній, однак, покладається на сторонні бази даних або платформи.

Обробка невизначеності – дві стратегії, які застосовуються в розглянутих моделях для обробки невизначеності. Це імовірнісна та порядкова стратегії. Дійсно, імовірнісний метод, який широко використовується, має чітко визначені математичні властивості. Крім того, порядкова міра представлена ранжуванням рівня придатності вектора атаки до використання. Фактично, цей рейтинг обирається за шкалою від 1 до 9, де 1 - найскладніший шлях.

Отриманий результат це два основних методи розрахунку ризику. Система або обчислює рівень можливості експлуатації (а не ризик), або використовує класичний спосіб, який враховує ймовірність експлуатації та показник потенційного впливу. Крім того, вибір методу, який обчислює ризик, передбачає, що моделі розробляються для загального застосування. Цей метод не враховує інші аспекти оцінки ризику, такі як фінансова інтерпретація, оцінка ризику з точки зору дотримання законодавства або з міркувань безпеки. Хоча в деяких публікаціях прямо не вказано, які рішення були підтримані, отримані

результати свідчать про те, що пріоритетність заходів захисту є ключовим результатом. Фактично, це підтверджує наш попередній висновок про те, що розглянуті методи мають загальний характер і не враховують пріоритетність інвестицій та дотримання законодавства.

Достовірність – це критерій, що вимірює здатність підходу відображати реальний рівень ризику. Дійсно, достовірність моделі оцінки ризику може бути виміряна як надійність та обґрунтованість. Якщо надійність стосується узгодженості результатів, то достовірність - їхньої точності порівняно з реальним ризиком, що лежить в основі моделі [103].

Більшість розглянутих методів зосереджені на підході, що базується на активах, хоча його вплив на роботу "розумних" міст все ще перебуває на початковій стадії. По-друге, втрата електроенергії внаслідок експлуатації електромережі може призвести до погіршення продуктивності системи управління дорожнім рухом. В той же час, розглянуті методи не враховують цю залежність. Однак точна оцінка впливу видається неможливою через брак емпіричних даних. Крім того, всі методи не враховують ризик використання інфраструктури як платформи для атак [104]. По-третє, оцінка в розглянутих роботах зосереджена на інфраструктурі та маніпулюванні даними, зі значним перекосом у бік першого класу. Однак дослідницькі та сторонні загрози є точками входу для багатьох атак, тоді як методи оцінки ризиків, схоже, недооцінюються (з точки зору їхньої значущості). По-четверте, розглянуті моделі вибирають імовірнісні та порядкові міри з найближчою частотою, знаючи, що теоретико-ігрові підходи рідко досліджуються. Нарешті, хоча в розглянутих роботах рідко вимірюється надійність (фактично, лише в одній моделі, запропонованій Фалько та ін. [69], результати порівнювалися з моделлю, створеною експертами), всі вони оминають вимірювання валідності.

2.7.3 Методи виявлення атак

Щоб оцінити ефективність розглянутих моделей, було виміряно наступні чотири метрики. Перша з них стосується здатності моделі правильно

класифікувати екземпляри, тоді як друга вимірює, наскільки добре модель може вловлювати патерни даних. Далі розглянемо прозорість моделі або наскільки процес вважається надійним. Остання метрика аналізує здатність підходу фіксувати атрибути виявлених загроз.

Здатність методу маркувати екземпляри можна представити як точність, достовірність, пригадування та F-міру. Дійсно, оцінка цих мір залежить від наступних показників.

– Достовірно позитивний результат (tp) вказує на те, що позитивний екземпляр класифіковано правильно.

– Істинно негативний (tn) означає, що негативний екземпляр класифіковано правильно.

– Хибнопозитивний (fp) вказує на те, що негативний екземпляр помилково класифіковано як позитивний.

– Хибно негативний (fn) означає, що позитивний екземпляр помилково класифіковано як негативний.

– Точність вважається основним показником правильності моделі виявлення. Вона обчислюється як відсоткове відношення всіх правильно класифікованих типів до всіх типів як $(tp + tn)/(tp + tn + fp + fn$ Однак точність може вводити в оману у випадку високого дисбалансу класів [105]. У цьому випадку для оцінки моделі необхідні наступні метрики.

– Точність вимірює частку правильно класифікованих примірників серед усіх записів, які класифікуються як позитивні. Вона визначається як $tp/(tp + fp)$. Дійсно, низька точність може вказувати на велику кількість fp.

– Відновлюваність, також відома як чутливість або істинно позитивна частота, являє собою відношення правильно класифікованих позитивних випадків до кількості випадків, які повинні бути класифіковані як позитивні. Формально вона визначається як $tp/(tp + fn)$. Насправді, низький відгук вказує на велику кількість fn.

– F-міра - це середнє гармонійне значення точності та пригадування. Вона визначається як $2 * tp/(2 * tp + fp + fn)$

Проблема зі здатністю моделі правильно класифікувати екземпляри полягає в тому, що вона не перевіряє роботу моделі на раніше не бачених даних. З цією метою ми оцінюємо, наскільки добре модель відображає шаблон даних. Насправді, існує декілька методів, які узагальнюють роботу моделі та допомагають оцінити здатність моделі вловлювати шаблони даних.

– Метод "утримання" випадковим чином ділить набір даних на дві підмножини, а саме: навчальну та тестову. Зазвичай це співвідношення становить 60/40, 70/30 або 80/20. Щоб уникнути ситуації, коли в підмножині виявляється нерівномірний розподіл класів, важливо збалансувати екземпляри, що належать до різних класів.

– k-кратна перехресна перевірка ділить набори даних на k підмножин; одна з них використовується як тестова множина, а інші k - 1 підмножин формують навчальну множину. Дійсно, метод гарантує, що кожен екземпляр є частиною тестової множини рівно один раз. Крім того, процес навчання та тестування моделі повторюється k разів, а для оцінки використовується середня помилка за всіма тестами. Однак, k-кратна перехресна перевірка є обчислювально дорогою, оскільки процес навчання та тестування має бути повторений k разів.

– Перехресна перевірка без пропусків - це k-кратна перехресна перевірка, де k дорівнює кількості екземплярів даних у наборі даних. Оцінка, отримана за допомогою цього методу, вважається хорошою, навіть якщо вона не є оптимальною з точки зору обчислень.

– Коефіцієнт кореляції Метьюса (MCC) враховує всі метрики з матриці класифікації, щоб зменшити вплив одного класу.

Крім того, моделі машинного навчання часто критикуються користувачами як "чорний ящик" через відсутність інтерпретованості, яка допомагає нам зрозуміти, як моделі приймають рішення на основі даних. З цією метою ми оцінюємо прозорість кожної моделі, дивлячись на те, як модель кількісно оцінює вплив кожного вхідного параметра, деталізує помилки моделі та записує результати на кожному кроці моделі. Дійсно, з різним рівнем деталізації, кілька робіт візуально пояснювали кроки запропонованих методів.

Однак майже 50% методів все ще залишаються незрозумілими. Насправді, зрозумілість моделі може підвищити довіру та практичне застосування. З огляду на це, слід надати більше пояснень щодо інтерпретованості результатів і самого процесу.

Численні моделі досягли точності понад 95%. Крім того, методи валідації та використані набори даних продемонстрували значний вплив на точність. Наприклад, більшість методів, які використовували штучні набори даних або змодельовані середовища, показали нижчу точність, ніж їхні аналоги, які використовували живі дані. Насправді, десятикратна перехресна перевірка показала вищу точність.

Розглянемо методи, які здатні фіксувати ознаки загроз. У цьому контексті оглянемо явні результати методів виявлення і оцінимо, як ці результати відповідають на наступні питання.

- Мета виявлення: яку атаку намагається виявити метод?
- Фаза атаки на якій фазі атаки метод виявляє вторгнення?
- Вектор атаки чи аналізує метод, яким чином було здійснено атаку?
- Атрибуція - чи пов'язує метод атаку з конкретним супротивником?
- Час виявлення (TTD) - скільки часу потрібно для виявлення атаки?
- Вплив - чи аналізує метод потенційний вплив атаки?

2.8 Відкриті питання та виклики

Крім того, в контексті розумних міст кіберзагрози та атаки, які спричиняються використанням різнорідних передових технологій, справді швидко розвиваються. Таким чином, нездатність управляти цими кіберзагрозами підриває довіру до зусиль, спрямованих на створення «розумних міст».

– Тому вкрай важливо визнати проактивний підхід для забезпечення безпеки на різних рівнях архітектури розумного міста. Крім того, з огляду на дефіцит бюджету, пов'язаного з безпекою, методи повинні визначати пріоритети витрат, щоб підвищити стійкість всієї екосистеми. Хоча деякі методи підтримують це імперативне завдання, є низка зауважень , які потребують уваги з боку дослідницької спільноти.

– Відсутність цілісної структури для ситуаційної обізнаності. Ситуаційна обізнаність у кіберпросторі є справді складним завданням. Фактично, розглянуті методи сприяють одному компоненту архітектури розумних міст без моделювання залежностей між ними. Крім того, схоже, не існує цілісного рішення для вирішення проблеми визначення пріоритетів у контексті конкретної інфраструктури (наприклад, енергетики, транспорту, охорони здоров'я тощо). Тому вкрай важливо розглядати виявлені загрози та поточні атаки в контексті функціонування «розумних міст» і розуміти їхній реальний вплив на критично важливі послуги. Однак взаємозв'язки не завжди є прямими. Тому розробка комплексного рішення вимагає міждисциплінарних досліджень.

– Підтримка аналізу ескалації загроз є складним завданням. Ескалація загроз повинна бути ретельно досліджена для підтримки кібер-рішень. Дійсно, є кілька рішень, які можуть допомогти у визначенні пріоритетів. По-перше, поєднання інформації щодо часу, необхідного для розслідування та усунення виявлених зловмисних подій. По-друге, ефективність раніше застосованих механізмів захисту від подібної проблеми. По-третє, аналіз витрат і вигод від пом'якшення наслідків. У цьому контексті можуть бути проведені додаткові дослідження для підтримки процесу прийняття рішень щодо безпеки розумних міст.

– Обмежена візуальна аналітика для ситуаційної обізнаності. Однією з найбільших проблем ситуаційної обізнаності є кількість і якість інформації, яку необхідно аналізувати. Хоча автоматизовані методи, засновані на машинному навчанні та обчислювальній потужності сучасних комп'ютерів, дозволяють ефективно обробляти дані, аналіз все ще вимагає людського судження, щоб зробити найкращу можливу оцінку результату та усунути негативний ефект суперечливих або неповних даних.

– Така інтеграція, відома як візуальна аналітика, значною мірою сприймається дослідницькою спільнотою [106]. Вона синтезує інформацію для отримання інсайтів та передачі оцінки для швидкого реагування. Використання людського пізнання для виявлення та відстеження прогресу загроз, оцінки допоміжної інформації та покращення процесу прийняття рішень у контексті «розумних міст», схоже, перебуває на початковій стадії розвитку.

– Оцінка моделей пріоритизації загроз є складним завданням. Однією з найважливіших проблем методів дослідження загроз в умовах розумних міст є їх оцінка. Дійсно, обмежена видимість залежностей між елементами всієї екосистеми, загрози, що постійно еволюціонують, і доступ до минулих інцидентів кібербезпеки ускладнюють встановлення істини в останній інстанції. Крім того, більшість розглянутих методів перевіряли результати за допомогою загальних ілюстративних сценаріїв. Відсутність зв'язку з реальними застосуваннями ставить під сумнів достовірність оцінених підходів. Крім того, надійність запропонованих методів також рідко вимірюється через брак емпіричних даних (для порівняння). Тому застосування польових стратегій, таких як інтерв'ю, експерименти та подібні дослідження, може допомогти у вирішенні завдання оцінювання.

– Дефіцит даних. Незважаючи на досягнення в галузі кібербезпеки, основна проблема узагальнення знань, отриманих з обмеженої колекції попередньо передбачуваних зловмисних подій, пов'язаних з «розумними містами», залишається невирішеною. Через відсутність у відкритому доступі вихідних даних про події та їхній вплив на різні аспекти «розумних міст», моделі оцінюються на основі даних, отриманих в лабораторних умовах.

2.9 Висновок до другого розділу

У цьому розділі були розглянуті методи та ідеї з огляду літератури. Було виділено і коротко описано використану теоретичну базу, вказуючи на категорії моделей, які її використовують. Також пов'язано моделі з виявленими загрозами, щоб проаналізувати охоплену сферу. Встановлено еталон для порівняння, вивчаючи основні характеристики базових даних і повідомляючи про декілька оціночних метрик.

Найбільше уваги було приділено загрозам, пов'язаним з інфраструктурою та даними. Проникнення в ресурси, включаючи облікові дані користувачів, досліджується рідко. Так само недостатньо вивчені такі загрози, як підробка даних і зловживання даними. Рідкісними винятками, розглянуті роботи які охоплюють одну категорію загроз, залишаючи інші загрози поза увагою. Крім того, обмежена сфера застосування може перешкоджати переходу до практичного застосування.

Розглянуті підходи зосереджуються на залежностях і підтримують високий рівень деталізації, де кожна сфера представлена як одна сутність. Це може свідчити про те, що кібернетичні взаємозалежності потребують додаткового підходу до моделювання для аналізу впливу кібератак, спрямованих на рівень даних. Розглянуті методи підтримують обмежену кількість доменів, що означає, що ці методи розроблені як доказ концепції, а можливість практичної реалізації вимагає подальшого дослідження. Масштабованість методу і його точність повинні бути ретельно розглянуті, навіть незважаючи на те, що методи оцінки точності залишаються недосконалими. Щоб відповідати загрозам, прокласифіковано сферу на основі чотирьох раніше визначених класів: розвідувальні загрози, диверсії інфраструктури, маніпуляції з даними та сторонні вразливості.

3 РЕАЛІЗАЦІЯ ЗАПРОПОНОВАНОЇ МОДЕЛІ

Розглянемо пропоновану гібридну модель глибокого навчання (DL) з точки зору структури, обраних алгоритмів DL та їх теоретичних концепцій. Запропонована модель глибокого навчання складається з моделей згорткової нейронної мережі (CNN) і квазірекурентної нейронної мережі (QRNN). QRNN. Вибрані моделі DL використовуються для класифікації типу загрози в реальному часі, забезпечуючи при цьому низьку FPR. Переваги використання CNN та QRNN полягають у тому, що вони дозволяють збільшити швидкість аналізу загроз при одночасному підвищенні точності класифікації. У решті цього розділу ми обговорюємо теоретичні концепції запропонованої моделі.

3.1 Згорткова нейронна мережа

Згорткова нейронна мережа (CNN) є розширенням нейронної мережі, запропонованої в роботі [107], і є ефективною для вилучення ознак на низькому рівні з вихідних даних, особливо просторових ознак [108]. CNN широко використовується в обробці зображень завдяки своїй здатності автоматизувати виділення ознак [109]. Крім того, CNN продемонстрував свою ефективність у багатьох сферах, таких як біомедичний аналіз текстів та класифікація шкідливих програм.

Залежно від форми вхідних даних, DL можна класифікувати на різні типи, включаючи двовимірні (2D) DL, які приймають такі дані, як зображення, та одновимірні (1D) DL, які приймають такі дані, як текстові дані. DL складається з шару згортки, шару об'єднання, шару повного з'єднання (FC) та функції активації [110]. Шар згортки є основним структурним елементом DL, який приймає два набори інформації як вхідні дані і виконує математичні операції над цими даними. Два набори інформації - це дані та фільтр, який можна назвати ядром. Фільтр застосовується до всього набору даних для створення карти ознак [109].

Рисунок 3.1 – Архітектура запропонованої гібридної моделі

Кожен фільтр CNN витягує набір ознак, карту ознак, яка на виході буде агрегована в нову карту ознак. Шар об'єднання реалізовано для зменшення розмірності карти ознак та видалення нерелевантних даних для покращення навчання. Вихідні дані шару об'єднання подаються до шару ФК для класифікації даних.

3.2 Квазірекурентна нейронна мережа (QRNN)

У роботі [113] запропоновано квазіконкурентну нейронну мережу (QRNN). Модель QRNN призначена для подолання обмеження конкурентної нейронної мережі з точки зору залежності обчислень на наступному кроці від попереднього кроку, що обмежує можливості паралелізму. QRNN використовує згорткові фільтри на вхідних даних і дозволяє довготривалу залежність послідовності для зберігання даних попередніх часових кроків [113]. Обчислювальна структура QRNN представлена на рис. 3.2.

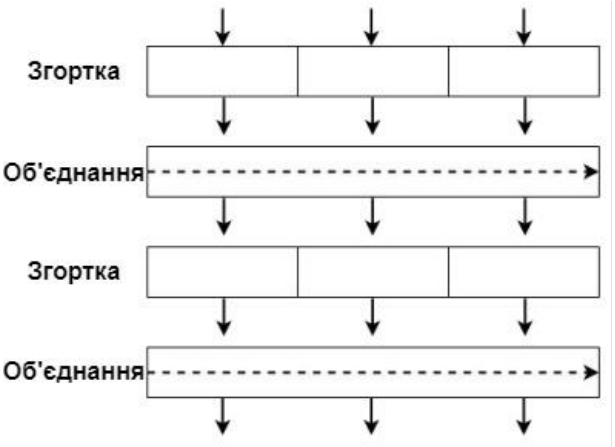

Рисунок 3.2 – Структура обчислень QRNN [123]

QRNN складається зі згорточних шарів і рекурентної функції об'єднання, які дозволяють QRNN працювати швидше, реєструючи 16-кратне збільшення швидкості [114]. Згортковий та об'єднувальний шари дозволяють проводити паралельні обчислення над пакетом та розмірністю ознак. QRNN використовується в різних додатках, таких як класифікація відео [112], синтез мови [114] та обробка природної мови [115].

3.3 Запропонована гібридна модель DL для кіберзагроз

Гібридна мережа глибокого навчання складається з шару 1D згортки, шару 1D максимального об'єднання, QRNN та FC шарів. Перший шар 1D згортки виділяє просторові особливості і створює карту особливостей, яка буде оброблена функцією активації. Функція активації (англ. Rectified Linear Unit, ReLU) використовується в згорткових шарах через її швидку збіжність градієнтного спуску, що робить її гарним вибором для запропонованої нами моделі [109]. Потім карта особливостей буде оброблена другим шаром, об'єднуючим шаром, для якого ми використали операцію максимального об'єднання. Операція максимального об'єднання вибирає максимальне значення в операції об'єднання [109]. Шар об'єднання зменшить розмірність і видалить нерелевантні ознаки. На виході CNN-моделі залишиться часова характеристика, яка буде вилучена за допомогою QRNN-моделі.

На рис. 3.3 показано деталі запропонованої нами моделі. Ми використовували два шари QRNN для вилучення часових ознак. У двох шарах QRNN прихований розмір представляє кількість прихованих одиниць, які також представляють вихідний розмір. Приховані одиниці можуть бути обрані до значення кількості ознак або вище [112]. Однією з проблем нейронної мережі є перенавчання, що означає, що модель занадто добре вивчає дані. Як наслідок, модель не зможе ідентифікувати варіанти в нових даних [116]. Таким чином, ми додали шар відсіву, щоб запобігти перенавчанню. Потім ми використали шар 1D згортки та шар максимального об'єднання, щоб виділити більше просторово-часових особливостей. Вихід моделі CNN передається на шар Flatten, який є

повністю пов'язаним вхідним шаром, що перетворює вихід шару об'єднання в один вектор, який є вхідним для наступного шару [117]. Нарешті, щільний шар, який також є повністю пов'язаним шаром, з функцією активації softmax використовується для класифікації загроз шляхом обчислення ймовірностей для кожного класу.

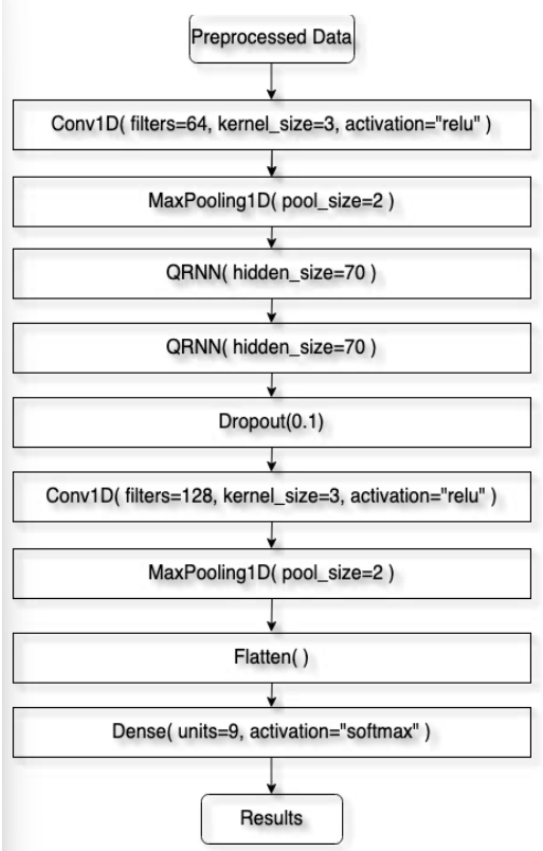

Рисунок 3.3 – Ілюстрація деталей запропонованої моделі [123]

3.4 Набори даних

У цій роботі ми вибрали наступні набори даних, оскільки вони змодельовані для представлення реалістичного середовища Інтернету речей, такого як "розумний дім" і "розумне місто", з точки зору різних аспектів:

- Неоднорідність змодельованих IoT-пристроїв, включаючи систему моніторингу погоди, розумне освітлення та розумний термостат.

- Різні сценарії ботнету, такі як зондування та DoS-атаки.

1) Набір даних про ботів та Інтернет речей

Для оцінки моделей ML використовуються різні набори даних, такі як KDD99, ISCX і CICIDS2017. Крім того, було створено кілька наборів даних, які відображають реалістичний мережевий трафік IoT для оцінки моделей машинного навчання для середовища IoT. Набір даних Bot-IoT використовується в судовому аналізі та для оцінки IDS. Набір даних містить звичайний трафік IoT і різні типи трафіку атак з підкатегоріями для кожного типу атак, які перераховані в Таблиці 3.1. Збір інформації або розвідка є однією із загроз конфіденційності, яка дозволяє зловмиснику збирати дані про жертву, наприклад, сканування портів і зняття відбитків пальців з операційної системи. Для DoS- та DDoS-атак використовувалися протоколи UDP, TCP та HTTP.

Таблиця 3.1 – Категорії атак у наборі даних bot-iot

Атака	**Підкатегорія**	**Кількість випадків**
Розпізнання	Сканування сервісів	73168
	OS відбитків пальців	17914
DoS	TCP	615800
	UDP	1032975
	HTTP	1485
DDoS	TCP	977380
	UDP	948255
	HTTP	989
Крадіжка інформації	Клавіатурне шпигунство	73
	Крадіжка даних	6

Набір даних був згенерований за допомогою віртуального стенду, який складається з трьох елементів: мережевих платформ, що використовують різні віртуальні машини, сервісів Інтернету речей, які моделюються за допомогою інструменту Node-red, що містить різні сервіси Інтернету речей, такі як метеостанція та функції вилучення даних, а також криміналістичної аналітики. Для оцінки запропонованої моделі ми використовували набір даних BoT-IoT для тестування поїздів.

2) Набір даних TON_IoT

Набір даних ToN_IoT - це один з найновіших наборів даних з кібербезпеки, який був створений в лабораторії Канберрського кібернетичного інституту. Набір даних був зібраний з тестової мережі IoT та промислового IoT (IIoT). Було використано набір даних тренувального тесту TON_IoT у форматі CSV. Набір даних містить загалом 461043 екземпляри та 9 типів атак, які представлені в Таблиці 3.2 із кількостю екземплярів для кожного типу.

Таблиця 3.2 – Категорії атак у наборі даних ton_iot

Атака	**Кількість випадків**
DoS	20000
DDoS	20000
Сканування	20000
Вимагачі	20000
Бекдор	20000
Ін’єкція	20000
Міжсайтовий скриптинг (XSS)	20000
Пароль	20000
Людина-посередник (MITM)	1043

3.5 Попередня обробка даних

Попередня обробка даних передбачає:

1) Видалення записи звичайного трафіку: В наборі даних Bot-IoT вирішено опустили функцію pkSeqID, оскільки вона являє собою ідентифікатор для записів трафіку.

2) Перетворення категорійних ознак: Набори даних містять деякі категоріальні ознаки, які не можуть бути оброблені нейронною мережею. Тому ми перетворили номінальні значення в числові за допомогою sklearn LabelEncoder. LabelEncoder перетворює категоріальні значення в числові.

3) Стандартизація даних: Багато моделей МН можуть погано працювати на наборах даних з високим розподілом даних. Таким чином, це вплине на ефективність навчання моделі [116]. Реалізовано sklearn StandardScaler для масштабування даних.

4) Розділення даних на навчальні та тестові: Для навчання та оцінювання було розділено дані на навчальні та тестові з співвідношенням 35% для тестування, враховуючи однакове співвідношення класів в обох частинах за допомогою параметра stratify.

3.6 Реалізація моделі

Параметри гібридної моделі, отримані на етапі навчання методом проб і помилок, включають кількість фільтрів CNN, кількість прихованих одиниць QRNN та частоту відсіву. Для розміру ядра найпоширенішими значеннями є 3 і 5, і розмір ядра 3 добре працює в цій роботі з обома наборами даних. розмір фільтра може допомогти у вилученні більшої кількості деталей з набору даних за рахунок збільшення кількості фільтрів. Таким чином, для першого шару CNN ми використали 64 фільтри, а для іншого шару CNN - 128 фільтрів.

3.7 Інструменти та показники оцінювання

Для оцінювання моделей МН важливо вибрати відповідні метрики оцінювання. Оцінки ефективності запропонованої моделі використовуються різні метрики оцінювання, зокрема точність, відношення помилково класифікованих даних (FPR), істинно позитивний результат (TPR), точність, пригадування та F-Score. Точність являє собою відношення кількості правильно класифікованих загроз до загальної кількості класифікованих загроз. FPR - це відношення помилково класифікованих даних до іншого типу загроз. В той час як TPR відображає здатність моделі правильно класифікувати загрози. Для оцінки загальної ефективності запропонованої моделі використовуються показники точності, пригадування та F-бали, де високе значення точності вказує на низький показник FPR. В той час як відгук відображає здатність моделі правильно класифікувати загрози. Наступні рівняння представляють метрики оцінки, де FP - хибнопозитивний результат, TP - істинно позитивний, TN - істинно негативний і FN - хибнонегативний.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3.1)$$

$$FPR = \frac{FP}{FP+FN} \quad (3.2)$$

$$TPR = \frac{TP}{TP+FP} \quad (3.3)$$

$$\text{Точність} = \frac{TP}{TP+FP} \quad (3.4)$$

$$\text{Повторність} = \frac{TP}{TP+FN} \quad (3.5)$$

$$\text{FScore} = \frac{2(\text{Точність}*\text{Повторність})}{(\text{Точність}+\text{Повторність})} \quad (3.6)$$

3.8 Оцінка та аналіз

У цьому розділі представлено результати та аналіз реалізації моделі. Для реалізації та оцінки ми використовували програмне забезпечення Jupyter Notebook з мовою програмування Python. Для попередньої обробки даних та реалізації запропонованої моделі ми використовували пакети Keras та scikitlearn. Ми протестували запропоновану модель на комп'ютері MacBook Air з процесором Intel Core i5 CPU 1,6 ГГц і 8 ГБ оперативної пам'яті. Також ми застосували різні сучасні ML-моделі на наборах даних, щоб порівняти їхню продуктивність із запропонованою нами моделлю.

На рис. 3.4 представлено матрицю помилок при використанні запропонованої нами моделі на наборі даних BoT-IoT. З рисунка видно, що модель правильно класифікувала більшість категорій кіберзагроз. Крім того, щоб проілюструвати якість запропонованої моделі, на рис. 3.5 для набору даних Bot-IoT побудована крива робочої характеристики приймача (ROC).

На рис. 3.6 представлена матриця помилок при використанні запропонованої моделі на наборі даних TON_IoT, а крива ROC представлена на рис. 3.7 для набору даних TON_IoT. На обох ROC-кривих запропонована нами модель досягла найвищого значення, яке дорівнює 1. Таким чином, запропонована нами модель дуже добре спрацювала з усіма класами.

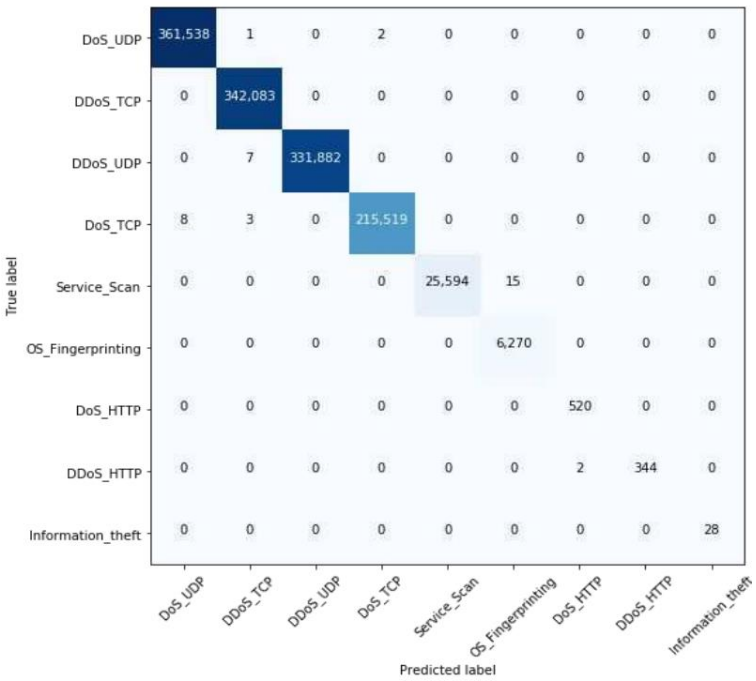

Рисунок 3.4 – Матриця класифікації на основі набору даних Bot-IoT [123]

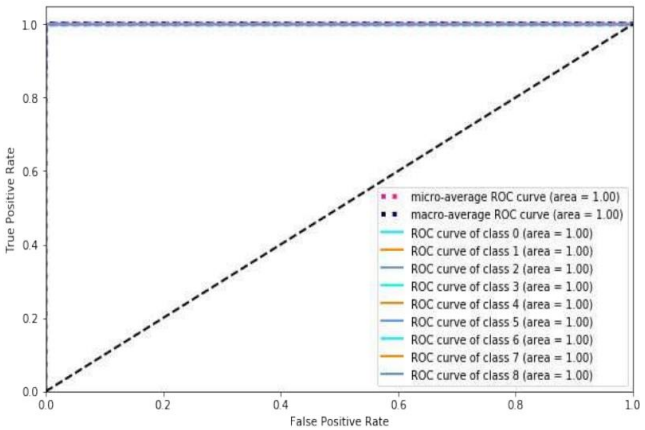

Рисунок 3.5 – ROC-крива використання запропонованої нами моделі на наборі даних Bot-IoT [123]

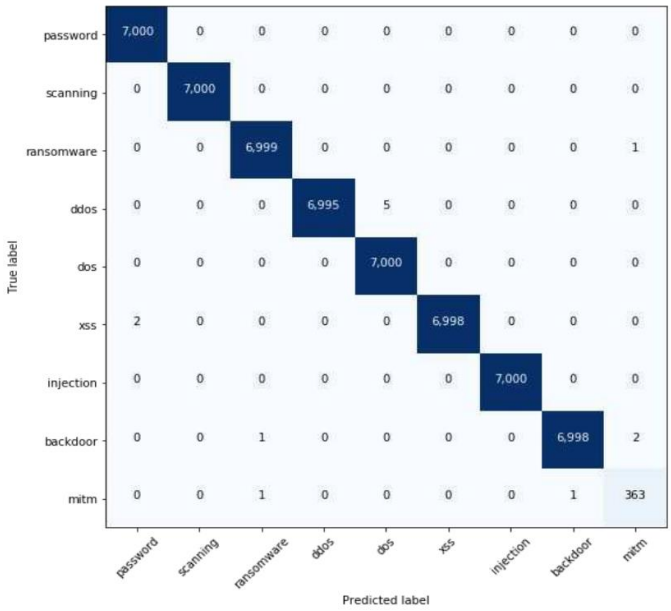

Рисунок 3.6 – Матриця класифікації на основі набору даних TON_IoT [123]

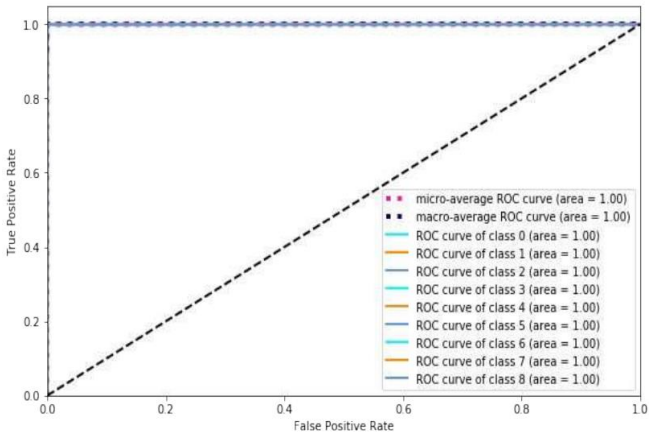

Рисунок 3.7 – ROC-крива використання запропонованої моделі на базі даних TON_IoT [123]

Результати застосування запропонованої нами моделі на тестових наборах даних наведено в 3.3.

Таблиця 3.3 – Результат класифікації кіберзагроз на обох наборах даних

Набір даних	**Точність%**	**TPR%**	**FPR**
BoT-IoT	99.99	99.92	0.0003
TON_IoT	99.99	99.99	0.001

Як показано в таблиці 3.3, запропонована модель досягає високої точності в середньому 99,99% на обох наборах даних. Так само, як і TPR, яка досягла в середньому 99,92% для набору даних BoTIoT і 99,99% для набору даних

TON_IoT. Щодо FPR, запропонована модель досягла низького FPR - 0,0003 для набору даних BoT-IoT та 0,001 для набору даних TON_IoT. Таким чином, запропонована модель показала хороші результати класифікації загроз з обома наборами даних. Щоб продемонструвати ефективність QRNN в нашій моделі, ми реалізували запропоновану модель з Довгою короткочасною памяттю (LSTM) замість QRNN, як представлено в Таблиці 3.4 і Таблиці 3.5.

Таблиця 3.4– Порівняння запропонованої нами моделі з використанням lstm та QRNN на основі набору даних bot-io.

Модель	**Точність**	**Повторність**	**F-Score**	**Середній час навчання**	**Час класифікації**
With LSTM	99.99%	100%	100%	1717.4 sec	sec
With QRNN	99.99%	100%	100%	1299.1 sec	sec

Таблиця 3.5 – Порівняння запропонованої нами моделі з використанням LSTM та QRNN на основі набору даних ton_iot..

Модель	**Точність**	**Повторгість**	**F-Score**	**Середній час навчання**	**Час класифікації**
With LSTM	99.99%	100%	100%	86.3 sec	sec
With QRNN	99.99%	100%	100%	66.5 sec	sec

Виходячи з результатів, наведених у Таблицях 3.4 і 3.5, запропонована нами модель з QRNN показала однакову продуктивність порівняно з запропонованою нами моделлю з LSTM з точки зору точності, точності, запам’ятовування та F-Score. З точки зору часу, запропонована модель з QRNN показала кращу продуктивність для навчання моделі та тестування. Таким чином, QRNN показав свою ефективність у збільшенні швидкості роботи моделі при забезпеченні високої точності та низького FPR. Отже, модель може бути використана в реальному часі. Також було порівняно продуктивність

запропонованої моделі на наборі даних Bot-IoT з найсучаснішими моделями для багатокласової класифікації загроз. Порівняння показано в таблиці 3.6.

Таблиця 3.6 – порівняння запропонованої нами моделі з сучасними моделями мультикласифікації на основі набору даних bot-iot

Рік	Точність%	Повторність%	F-Score%
2019	99.00	99.00	99.00
2019	99.97	-	95.7
2020	99.80	99.00	98.80
2020	99.99	100	100

Як показано в Таблиці 3.6, модель перевершила інші моделі. Крім того, реалізовано різні моделі ML, щоб порівняти їх продуктивність з нашою моделлю. Точність, TPR та FPR кожної моделі з нашою моделлю наведено в Таблиці 3.7 та Таблиці 3.8. Запропонована модель показала кращі результати, ніж інші чотири моделі, завдяки поєднанню CNN з QRNN.

Таблиця 3.7 – Порівняння запропонованої моделі з іншими моделями ml на основі набору даних bot-iot

Модель	Точність%	TPR%	FPR
MLP	99.98	86.42	0.002
CNN	99.98	88.13	0.001
GRU	99.98	96.06	0.001
LSTM	99.99	94.69	0.0004
Сформована модель	99.99	99.92	0.0003

Таблиця 3.8 – Порівняння запропонованої моделі з іншими моделями ml на основі набору даних ton_iot

Model	Accuracy%	TPR%	FPR
MLP	99.67	99.51	0.03
CNN	99.88	99.75	0.01
GRU	97.85	96.95	0.27
LSTM	99.83	99.79	0.02
Сформована модель	99.99	99.99	0.001

3.9 Висновок до третього розділу

У цьому розділі описано набори даних, які ми відібрали для оцінки запропонованої моделі. Розглянуто кроки попередньої обробки даних, процес вибору параметрів моделі та обрані метрики оцінювання. Цей розділр є важливим для розробки та використання квазіконкурентних нейронних мереж (QRNN) для подолання обмежень, пов'язаних з конкурентними нейронними мережами. Модель QRNN вирізняється здатністю подолати обмеження щодо залежності обчислень між послідовними кроками, що розширює можливості паралелізму. Застосування згорткових фільтрів на вхідних даних дозволяє використовувати довготривалу залежність послідовності для зберігання інформації від попередніх часових кроків.

На етапі навчання було отримано параметри гібридної моделі, які включають кількість фільтрів CNN, кількість прихованих одиниць QRNN та частоту відсіву. Важливим аспектом є також розмір ядра фільтра, де зауважується, що розмір ядра 3 показав хороші результати з обома наборами даних. Розмір фільтра має вплив на вилучення деталей з набору даних, і в цій роботі використовувалось 64 фільтри для першого шару CNN та 128 фільтрів для другого шару CNN.

Отже, використання QRNN з зазначеними параметрами дозволяє ефективно вирішувати завдання, пов'язані з довготривалими залежностями та обмеженнями конкурентних нейронних мереж, підкреслюючи важливість оптимізації параметрів для досягнення найкращих результатів.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Питання щодо охорони праці

Тема дослідження тісно пов’язана з ІТ індустрією, тому доцільно розглянути питання щодо методи оцінки ризиків, що виникають в ІТ та управління ними. В Україні з’являється дослідницький інтерес до тих галузей народного господарства, які в найближчому майбутньому будуть високо конкурентними на світових ринках. Одним із таких напрямів є ІТ-індустрія, яка незалежно від складних умов, продовжує залучати іноземні інвестиції та створювати в країні робочі місця. ІТ-сектор України продовжує своє зростання більш високими темпами, ніж економіка країни в [118]. Завдяки українським ІТ-фахівцям, які працюють сьогодні на західних замовників, Україна може перетворитися на найбільший технологічний центр світу. Фахівці з України розробляють програмне забезпечення для найскладніших медичних приладів, військової техніки, автомобілів майбутнього, освоєння космосу тощо [119].

Отже, ІТ-галузь дуже швидко набуває стадії зрілості. Це призводить до поступового посилення конкуренції в усіх її сегментах, причому компанії змагаються не лише за долю на ринку, а й за інвестиції та персонал. Для того, щоб залишатися висококонкурентними, компаніям доводиться переглядати свої стратегії в конкурентній боротьбі і шукати ефективні рішення формування конкурентних переваг.

Стан конкуренції в сегменті, згідно теорії М. Портера, залежить від дії п’яти основних конкурентних сил: ризик появи товарів-субститутів, внутрішньогалузеві загрози конкуренції, проникнення нових конкурентів, загроза (ризик) втрати клієнтів, загроза (ризик) нестабільності постачальника. Основними показниками, що визначають дію п’яти конкурентних сил, є: умови попиту; виробничі умови; характер стратегії компанії; наявність підтримуючих або пов’язаних галузей .

"Модель п’яти сил (напрямів) конкуренції – це ефективний метод аналізу основних конкурентних сил, що впливають на положення фірми на ринку. Ця

модель дає можливість більш цілеспрямовано оцінити конкурентний стан на ринку і на цій основі розробити такий варіант довгострокової стратегії фірми, який в найбільшій мірі забезпечить її захист і одночасно сприятиме створенню додаткових конкурентних переваг". Практичне застосування моделі Портера припускає проходження двох етапів. Перший – оцінка тиску кожної з п’яти сил на позиції підприємства; другий – вибір відповідної стратегії реакції.

Проведений аналіз дозволив зробити висновок про те, що компаніям необхідно звертати основну увагу на виробництво нового продукту і правильне його позиціонування. Диференціація ІТ-продуктів грає в даному випадку важливу роль, оскільки це допомагає компаніям надати своєму своїм розробкам специфічні риси, які відрізняють їх від конкуруючих компаній, і сприяє залученню більшої кількості покупців. Таким чином, конкуренція між компаніями на ринку ІТ-послуг визначається значною мірою впливом галузевої конкуренції, ринковою владою покупців і загрозою появи товарів замінників, що, у свою чергу, є стимулом для розробки нових стратегій диференціації продукту і фокусуванні на збільшенні прибутку і утриманні користувачів. При цьому необхідно звертати особливу увагу на те, що диференціація продукту на ринку ІТ-послуг має на увазі значні фінансові вкладення, які спрямовуються на формування компетентності для виробництва комплексних послуг за допомогою інвестицій в навчання і підвищення кваліфікації персоналу, а також сертифікації фахівців і отримання досвіду в реалізації масштабних проектів. Тому диференціація продукту на ринку ІТ-послуг в довгостроковій перспективі – це можливість забезпечити відносно безпечне майбутнє компаній. Посилення конкурентної позиції компанії неможливе без зниження (мінімізації) ризиків, що притаманні її діяльності.

Можна виділити п’ять груп ризиків, що мають досить високу ймовірність виникнення, а саме: політичні, економічні, операційні та юридичні, та визначити рівень основних ризиків компанії. В сучасних умовах базою для управління ризиком є концепція прийнятного ризику, що передбачає ефективне зниження рівня ризику та доводить його до прийнятного стану. Як правило, першочергові заходи реагування на ризик – контроль за ходом діяльності і процесами

організації. Це знижує рівень ризику, але якщо залишковий ризик все ж вище, ніж прийнятний для організації, то необхідно передбачити спеціальні заходи реагування на ризик. Управління ризиком в організації мають здійснювати спеціалізовані підрозділи або підсистема (система) управління ризиками (СУР) в системі управління підприємством. Якщо компанія не має СУР взагалі, то вже тільки це є серйозним стратегічний ризиком. Модель інформаційного забезпечення СУР IT-компанії дозволить сформувати необхідну базу, для подальшого формування і розвитку процесів аналізу IT-ризиків. Оптимально побудовані процеси аналізу ризиків дозволяють закласти міцний, надійний, але в той же час відносно гнучкий інформаційний фундамент, на якому стає можливим побудувати надійний домен інформаційних технологій, що забезпечує організації якісним і відносно "безризиковими" процесами [120].

Отже, проведений аналіз дозволяє зробити наступні висновки та надати підприємствам IT-галузі такі рекомендації:

1) дотримуватися стратегії диференціації, тобто зміцнення унікальності продукту і зосереджуватись на такому цільовому ринку, для якого важливі унікальні характеристики. Конкурентна стратегія – стратегія лідерства продукту;

2) основні зусилля зосереджувати на створенні високого рівня знань про продукти та підвищення обізнаності про унікальні особливості продукту;

3) щоб зберегти конкурентоспроможність, необхідно постійно стежити за пропозиціями конкурентів та появою нових гравців;

4) посилення лідерських позицій, що буде заважати проникненню нових конкурентів на ринок;

5) концентрувати діяльність на побудові довгострокових та стабільних відносин з клієнтами;

6) позиціонувати себе як відомий бренд, який може гарантувати якість і високий рівень обслуговування.

4.2 Питання щодо безпеки в надзвичайних ситуаціях

Тема кваліфікаційної роботи присвячена кіберзагрозам у «розумному місті», в «розумному місті» доцільно розглянути питання створення і функціонування системи моніторингу довкілля з метою інтеграції екологічних інформаційних систем, що охоплюють певні території.

У документах міжнародної конференції ООН з питань довкілля (Стокгольм, 1972) була висунута ідея моніторингу в формі національних систем постійного спостереження за зміна-ми в біосфері з метою одержання достовірних відомостей зростання техногенного впливу на її компоненти, екологічного прогнозування і обґрунтування рішень щодо регулювання взає-модії техносфери з біосферою.

Моніторинг (від лат. monitor – той, що наглядає, нагадує) – слідкування за якимись об’єктами або явищами; постійне і безперервне спостереження; у застосуванні до сере-довища життя – моніторинг оточуючого людину середовища: спостереження, оцінка (порівняння з нормативними параметрами) і прогноз стану довкілля, попередження про можливі критичні ситуації, шкідливі чи небезпечні для здоров’я людини та інших живих організмів.

Отже, сутність моніторингу полягає у спостереженні за довкіллям, оцінюванні його фактичного стану, прогнозуванні його розвитку. За міжнародним стандартом (СТ ІСО 4225-80), моніторинг – це багаторазове вимірювання для спостереження за змінами будь-якого параметра в певному інтервалі часу; система тривалих спостережень, оцінювання, контро-лювання й прогнозування стану і зміни об'єктів. Крім спостережень і отримання інформації, моніторинг передбачає і елементи активних дій, таких як оцінювання, прогнозування, роз-роблення природоохоронних рекомендацій.

Моніторинг довкілля – система спостереження і контролю за природними, природ-но-антропогенними комплексами, процесами, що відбуваються у них, навколишнім се-редовищем загалом з метою раціонального використання природних ресурсів і охорони довкілля, прогнозування масштабів неминучих змін.

Як галузь екологічної науки, моніторинг довкілля ґрунтується на загальних екологіч-них законах і взаємодіє з природничими, географічними і технічними науками. Його за-вдання полягають у постановці й виробленні теоретичних засад практичного розв'язання проблем організації спостережень; науковому обґрунтуванні складу, структури мережі й ме-тодів спостережень за природним фоном, природними явищами, планетарними процесами, рівнем забруднення середовищ, станом біоти (сукупності живих організмів, що населяють певний район у певний проміжок часу), фізичними параметрами біосфери; виборі методів, методик оцінювання і прогнозування стану довкілля; розробленні рекомендацій щодо уп-равління станом складових біосфери. Отже, система моніторингу довкілля надає інформацію науковцям і практикам для конструктивного вирішення екологічних проблем і тому є інформаційною основою сучасної екології.

Моніторинг НПС є системою моніторингів різного рівня, основу яких утворюють ба-зові компонентні та ресурсні моніторинги:

1) біоекологічний (лісоекологічний, степової рослинності, тваринного світу, гідробіо-логічних систем);

2) літоекологічний (ґрунтовий, геохімічної ситуації, інженерно-екологічної обстановки, повітряного і гідрогеологічного середовищ, умов добування корисних копалин, глибинних шарів літосфери);

3) гідроекологічний (рік і водосховищ, озер і боліт, гирл річок, лиманів і естуаріїв, мо-рів і океанів);

4) екології атмосфери (нижнього шару, високих шарів, місцевого середовища і закри-тих приміщень);

5) соціально-економічний (міждержавний, державний, муніципальний, підприємства, ринку).

Крім базового рівня моніторингів можна виділити ще два рівні:

1) спеціальний (радіаційний, озоновий, пестицидний);

2) комплексний відомчий (агроекологічний, лісогосподарський, водогосподарський, санітарно-гігієнічний та ін.) та комплексний територіальний (урбанізованих і рекреаційних зон, міст, технополісів тощо).

Національні й регіональні геоінформаційні системи моніторингового типу давно функціонують у багатьох країнах. Їхній досвід може бути особливо корисний у контексті розробки, впровадження й удосконалення системи екологічного моніторингу в Україні Цей досвід свідчить, що для вирішення даної проблеми потрібні:

1) формування самостійного напряму науково-технічних робіт і виробничої діяльності з метою налагодження і виробництва контрольно-аналітичних приладів і апаратури, які забезпечують інструментальне спостереження за перебігом еколого-економічних процесів і станом довкілля;

2) розробка національної системи показників і стандартів якості довкілля та загальнодоступних методів їхнього вимірювання;

3) створення оптимальної мережі контрольно-вимірювальних станцій на локальному, регіональному і національному рівнях, а також обов’язкове впровадження уніфікованих систем статистичної звітності про стан еколого-економічної ситуації і тенденції її зміни.

З метою забезпечення збору, обробки, збереження та аналізу інформації про стан до-вкілля, прогнозування його змін та розробки науково обґрунтованих рекомендацій для прийняття ефективних управлінських рішень в Україні з 1991 р. почали створювати систему державного моніторингу навколишнього природного середовища (НПС) [121].

Під час дослідження стану довкілля використовують методи якісного (діагностують на-явність певного хімічного елемента, сполуки) і кількісного (визначають кількість (концент-рацію) хімічного елемента, сполуки у довкіллі) аналізів довкілля. Залежно від параметрів, які підлягають вимірюванню, методи кількісного аналізу поділяють на хімічні, фізико-хімічні, фізичні та біологічні. Вибір конкретного методу дослідження залежить від вмісту аналізова-ної речовини і хімічного складу досліджуваного об'єкта [122].

4.3 Висновок до четвертого розділу

В третьому розділі кваліфікаційної роботи описується збільшений інтерес до дослідження та управління ризиками в галузі інформаційних технологій (ІТ). Зростання конкуренції в ІТ-галузі ставить перед компаніями завдання переглядати свої стратегії та шукати ефективні рішення для формування конкурентних переваг. Ризики, пов'язані з політичними, економічними, операційними та юридичними аспектами, розглядаються як важливий елемент управління організацією, існує концепція прийнятного ризику для зниження рівня ризику до прийнятного рівня.

В умовах зростаючого інтересу до охорони довкілля в Україні обговорюється питання створення і функціонування системи моніторингу довкілля. Моніторинг довкілля визначається як система спостереження і контролю за природними та природно-антропогенними комплексами з метою раціонального використання ресурсів та охорони навколишнього середовища.

Як для галузі ІТ, так і для охорони довкілля, ефективне управління ризиками та впровадження систем моніторингу є ключовими аспектами для забезпечення стабільності, конкурентоспроможності та сталого розвитку організацій в умовах швидкозмінного оточення.

ВИСНОВКИ

У цій кваліфікаційній роботі розглянуто ключові питання: ландшафт кіберзагроз у «розумних містах», методи, засновані на даних, для розробки можливостей ситуаційної обізнаності, методи, засновані на вимірюваннях, які використовуються для порівняння обсягу та ефективності кожного методу. Стійкість розглянутих методів до різних ідентифікованих кіберзагроз.

Решта цього дослідження організована наступним чином. У наступному розділі ми розглядаємо пов'язані дослідження і демонструємо додаткову цінність запропонованого дослідження. У розділі "Розумні міста: архітектура та ландшафт загроз" ми представляємо функціональну архітектуру розумних міст і вказуємо на кілька поширених кіберзагроз, пов'язаних з ними. У розділі "Методи підтримки кіберситуаційної обізнаності" ми описуємо вибрані методи виявлення, а в розділі "Обговорення та основні висновки" ми відповідно оцінюємо їх з різних точок зору. У розділі "Відкриті питання та перспективи на майбутнє" ми обговорюємо поточні дослідження, розробки та оперативні виклики, пропонуючи можливі майбутні дослідницькі ініціативи, спрямовані на вдосконалення наявної аналітики для захисту від кіберзагроз. Нарешті, у розділі "Висновки" ми підсумовуємо внесок кожного розділу цього дослідження.

Виходячи з цього, можемо запропонувати класифікацію кіберзагроз і навести ілюстративні приклади атак та їх вплив на роботу «розумних міст». Надати багатовимірну оцінку наявних методів, які підтримують кіберситуаційну обізнаність в контексті «розумних міст» і технологій, що їх підтримують. В роботі розглядається класифікація методів на основі аналізу теоретичних моделей, що лежать в їх основі, відповідних даних, а також їх технологічна та контекстна сфера застосування. У ньому також обговорюються кілька критеріїв оцінювання та їхня візуальна підтримка (або відсутність такої).

Загалом робота розглядає проблеми кібербезпеки в контексті «розумних міст» та визначає чотири основних класи загроз: дослідницькі загрози, саботаж інфраструктури, маніпуляції з даними та вразливості третіх сторін. Аналізується вразливість існуючої інфраструктури до традиційних та нових кіберзагроз, таких як віруси, підслуховування, атаки на дані, та використання алгоритмів

машинного навчання. Особлива увага приділяється нестачі комплексних досліджень методів підтримки кіберситуаційної обізнаності в розумних містах.

Огляду досліджень, вказує на недостатність досліджень щодо загроз, пов'язаних з підробкою та зловживанням даними, а також обмежену сферу застосування. Для подолання обмежень конкурентних мереж визначено параметри гібридної моделі та підкреслено важливість їх оптимізації, досягнення найкращих результатів. Цей підхід дозволяє ефективно вирішувати завдання, пов'язані з довготривалими залежностями в данних.

Робота виявляє важливість подальших досліджень у сфері кібербезпеки «розумних міст» та розвитку оптимальних методів для виявлення та подолання різноманітних кіберзагроз.

В першому розділі кваліфікаційної роботи освітнього рівня «Магістр»:

– Подано архітектуру «розумного міста»

– Розглянуто кіберзагрози для «розумного міста»

В другому розділі кваліфікаційної роботи:

– Описано моделі взаємозалежності та оцінку ризиків загроз.

– Досліджено методи виявлення атак

– Подано порівняльний опис показників порівняння та оцінки моделей

В третьому розділі кваліфікаційної роботи:

– Запропоновано реалізація гібридної моделі виявлення кіберзагроз

– Протестовано квазіконкурентну нейронну мережу, подано відповідні набори даних та їх реалізованої їх обробку.

У розділі «Охорона праці та безпека в надзвичайних ситуаціях» проаналізовано методи оцінки ризиків, що виникають в ІТ та питання створення і функціонування системи моніторингу довкілля з метою інтеграції екологічних інформаційних систем.

ПЕРЕЛІК ДЖЕРЕЛ

1 United Nations. 68% of the world population projected to live in urban areas by 2050. 2018. https ://www.un.org. Дата доступу: 20.11.23.

2 City Profile. Smart cities world. https ://www.smart citiesworld.net. Дата доступу: 20.11.23.

3 Singapore uses IoT to create smart buildings. 2016. www.smart -energy.com Дата доступу: 20.11.23.

4 Building a smart + equitable city. The official website of the City of New York. 2015. f. Дата доступу: 20.11.23.

5 IBM. City of Rio de Janeiro and IBM collaborate to advance emergency response system; access to real-time information empowers citizens. 2011. https ://www.prnew swire .com/ Дата доступу: 20.11.23.

6 Mclaughlin T. As shootings soar, Chicago police use technology to predict crime. 2017. https ://www.reute rs.com/ Дата доступу: 20.11.23.

7 The Register. Sweden ‘secretly blames’ hackers—not solar flares—for taking out air traffic control. The Register. 2018. https ://www.theregiste r.co.uk Дата доступу: 20.11.23.

8 Case DU. Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), vol. 388, 2016.

9 Kraszewski K. SamSam and the Silent Battle of Atlanta. In: 2019 11th international conference on cyber conflict (CyCon), 2019. vol. 900, p. 1–16.

10 Kan M. Ransomware strikes Baltimore’s 911 dispatch system. PCMag Asia. 2018. https ://sea.pcmag.com Дата доступу: 20.11.23.

11 Mettler K. Somebody keeps hacking these Dallas road signs with messages about Donald Trump Bernie Sanders and Harambe the gorilla. Washington, DC: WP Company; 2019.

12 Dallas warning sirens “set off by hacker”. BBC. 2017.

13 Khan R, Kumar P, Jayakody DNK, Liyanage M. A survey on security and privacy of 5G technologies: potential solutions, recent advancements and future directions. IEEE Commun Surv Tutor. 2019;22(1):196–248.

14 Chan L, et al. Survey of AI in cybersecurity for information technology management. In: 2019 IEEE technology & engineering management conference (TEMSCON). 2019. p. 1–8.

15 Druzdzel MJ, Flynn RR. Decision support systems. In: Encyclopedia of library and information sciences. Boca Raton: CRC Press; 2017. p. 1200–8.

16 Ijaz S, Shah MA, Khan A, Ahmed M. Smart cities: a survey on security concerns. Int J Adv Comput Sci Appl. 2016;7(2):612–25.

17 Gharaibeh A, et al. Smart cities: a survey on data management, security, and enabling technologies. IEEE Commun Surv Tutor. 2017;19(4):2456–501.

18 Silva BN, Khan M, Han K. Towards sustainable smart cities: a review of trends, architectures, components, and open challenges in smart cities. Sustain Cities Soc. 2018;38:697–713.

19 Baig ZA, et al. Future challenges for smart cities: cyber-security and digital forensics. Digit Investig. 2017;22:3–13.

20 Cui L, Xie G, Qu Y, Gao L, Yang Y. Security and privacy in smart cities: challenges and opportunities. IEEE;6:46134–45.

21 Sookhak M, Tang H, He Y, Yu FR. Security and privacy of smart cities: a survey, research issues and challenges. IEEE Commun Surv Tutor. 2019;21(2):1718–43. https ://doi.org/10.1109/COMST .2018.28672 88.

22 Talari S, Shafie-Khah M, Siano P, Loia V, Tommasetti A, Catalão JP. A review of smart cities based on the internet of things concept. Energies. 2017;10(4):421.

23 Banerjee J, Das A, Sen A. A survey of interdependency models for critical infrastructure networks. ArXiv Prepr. ArXiv170205407. 2017.

24 Tøndel IA, Foros J, Kilskar SS, Hokstad P, Jaatun MG. Interdependencies and reliability in the combined ICT and power system: an overview of current research. Appl Comput Inform. 2018;14(1):17–27.

25 Kitchin R, Dodge M. The (in) security of smart cities: vulnerabilities, risks, mitigation, and prevention. J Urban Technol. 2019;26(2):47–65.

26 Vitunskaite M, He Y, Brandstetter T, Janicke H. Smart cities and cyber security: are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Comput Secur. 2019;83:313–31.

27 Habibzadeh H, Nussbaum BH, Anjomshoa F, Kantarci B, Soyata T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustain Cities Soc. 2019;50:101660.

28 Mehmood Y, Ahmad F, Yaqoob I, Adnane A, Imran M, Guizani S. Internet-of-things-based smart cities: recent advances and challenges. IEEE Commun Mag. 2017;55(9):16–24. https ://doi.org/10.1109/MCOM.2017.16005 14.

29 Galluscio M, et al. A first empirical look on internet-scale exploitations of IoT devices. In: 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC). 2017. p. 1–7.

30 Ercolani VJ, Patton MW, Chen H. Shodan visualized. In: 2016 IEEE conference on intelligence and security informatics (ISI). 2016. p. 193–5.

31 Patton M, Gross E, Chinn R, Forbis S, Walker L, Chen H. Uninvited connections: a study of vulnerable devices on the internet of things (IoT). In: 2014 IEEE joint intelligence and security informatics conference. 2014. p. 232–5.

32 PALO ALTO NETWORKS. Impacts of cyberattacks on IoT devices. www.sdxcentral.com Дата доступу: 20.11.23.

33 Sicato S, Costa J, Sharma PK, Loia V, Park JH. VPNFilter malware analysis on cyber threat in smart home network. Appl Sci. 2019;9(13):2763.

34 Zimba A, Wang Z, Mulenga M. Cryptojacking injection: a paradigm shift to cryptocurrency-based web-centric internet attacks. J Organ Comput Electron Commer. 2019;29(1):40–59.

35 Bou-Harb E, Debbabi M, Assi C. A novel cyber security capability: inferring internet-scale infections by correlating malware and probing activities. Comput Netw. 2016;94:327–43.

36 Bertino E, Islam N. Botnets and internet of things security. Computer. 2017;50(2):76–9.

37 Kumar M. DDoS attack takes down central heating system amidst winter in Finland. The Hacker News. 2016. https ://thehackern ews.com. Дата доступу: 20.11.23.

38 Trappe W, Howard R, Moore RS. Low-energy security: limits and opportunities in the internet of things. IEEE Secur Priv. 2015;13(1):14–21.

39 Georgiou K, Xavier-de-Souza S, Eder K. The IoT energy challenge: a software perspective. IEEE Embed Syst Lett. 2017;10(3):53–6.

40 Mohurle S, Patil M. A brief study of wannacry threat: ransomware attack 2017. Int J Adv Res Comput Sci. 2017. https ://doi.org/10.26483 /IJARC S.V8I5.4021.

41 Ransomware attack on San Francisco public transit gives everyone a free ride. The Guardian. 2016. Доступно: www.thegu ardian.com Дата доступу: 20.11.23.

42 Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur TISSEC. 2011;14(1):1–33.

43 Liang G, Zhao J, Luo F, Weller SR, Dong ZY. A review of false data injection attacks against modern power systems. IEEE Trans Smart Grid. 2016;8(4):1630–8.

44 Wurm J, Hoang K, Arias O, Sadeghi AR, Jin Y. Security analysis on consumer and industrial IoT devices. In: 2016 21st Asia and South Pacific design automation conference (ASP-DAC). 2016. p. 519–24.

45 Van Zoonen L. Privacy concerns in smart cities. Gov Inf Q. 2016;33(3):472–80.

46 Usama M, Asim M, Latif S, Qadir J, et al. Generative adversarial networks for launching and thwarting adversarial attacks on network intrusion detection systems. In: 2019 15th international wireless communications & mobile computing conference (IWCMC). 2019. p. 78–83.

47 Lin P, Swimmer M, Urano A, Hilt S, ve Vosseler R (2017) Securing smart cities moving toward utopia with security in mind. A TrendLabs Research Paper, Erişim Tarihi: 15 Eylül 2019.

48 Laugé A, Hernantes J, Sarriegi JM. Critical infrastructure dependencies: a holistic, dynamic and quantitative approach. Int J Crit Infrastruct Prot. 2015;8:16–23.

49 König S, Rass S. Investigating stochastic dependencies between critical infrastructures. Int J Adv Syst Meas. 2018;11:250–8.

50 Stergiopoulos G, Kotzanikolaou P, Theocharidou M, Gritzalis D. Risk mitigation strategies for critical infrastructures based on graph centrality analysis. Int J Crit Infrastruct Prot. 2015;10:34–44.

51 Stergiopoulos G, Kotzanikolaou P, Theocharidou M, Lykou G, Gritzalis D. Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures. Int J Crit Infrastruct Prot. 2016;12:46–60.

52 Beccuti M, Chiaradonna S, Di Giandomenico F, Donatelli S, Dondossola G, Franceschinis G. Quantification of dependencies between electrical and information infrastructures. Int J Crit Infrastruct Prot. 2012;5(1):14–27.

53 Bloomfield RE, Popov P, Salako K, Stankovic V, Wright D. Preliminary interdependency analysis: an approach to support critical-infrastructure risk-assessment. Reliab Eng Syst Saf. 2017;167:198–217.

54 Netkachov O, Popov P, Salako K. Quantification of the impact of cyber attack in critical infrastructures. In: International conference on computer safety, reliability, and security. 2014. p. 316–27.

55 Johansen C, Tien I. Probabilistic multi-scale modeling of interdependencies between critical infrastructure systems for resilience. Sustain Resilient Infrastruct. 2018;3(1):1–15.

56 Heracleous C, Kolios P, Panayiotou CG, Ellinas G, Polycarpou MM. Hybrid systems modeling for critical infrastructures interdependency analysis. Reliab Eng Syst Saf. 2017;165:89–101.

57 Ferdowsi A, Saad W, Maham B, Mandayam NB. A Colonel Blotto game for interdependence-aware cyber-physical systems security in smart cities. In: Proceedings of the 2nd international workshop on science of smart city operations and platforms engineering. 2017. p. 7–12.

58 Li Z, Jin D, Hannon C, Shahidehpour M, Wang J. Assessing and mitigating cybersecurity risks of traffic light systems in smart cities. IET Cyber Phys Syst Theory Appl. 2016;1(1):60–9.

59 Kelarestaghi KB, Foruhandeh M, Heaslip K, Gerdes R. Intelligent transportation system security: impact-oriented risk assessment of in-vehicle networks. IEEE Intell Transp Syst Mag. 2019. https ://doi.org/10.1109/MITS.2018.28897 14.

60 Kotzanikolaou P, at all. Assessing n-order dependencies between critical infrastructures. Int J Crit Infrastruct. 2013;9(1–2):93–110.

61 Neshenko N, Bou-Harb E, Crichigno J, Kaddoum G, Ghani N. Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Commun Surv Tutor. 2019;21(3):2702–33.

62 Sicari S, Rizzardi A, Miorandi D, Coen-Porisini A. A risk assessment methodology for the internet of things. Comput Commun. 2018;129:67–79.

63 Wang H, Chen Z, Zhao J, Di X, Liu D. A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow. 20;6:8599–609.

64 Mell P, Scarfone K, Romanosky S. Common vulnerability scoring system. IEEE Secur Priv. 2006;4(6):85–9.

65 Radanliev P, et al. Future developments in cyber risk assessment for the internet of things. Comput Ind. 2018;102:14–22.

66 Mohammad N. A multi-tiered defense model for the security analysis of critical facilities in smart cities. 2019;7:152585–98.

67 Shivraj V, Rajan M, Balamuralidhar P. A graph theory based generic risk assessment framework for internet of things (IoT). In: 2017 IEEE international conference on ANTS. 2017. p. 1–6.

68 Mohsin M, Sardar MU, Hasan O, Anwar Z. IoTRiskAnalyzer: a probabilistic model checking based framework for formal risk analytics of the internet of things. IEEE;5:5494–505.

69 Falco G, et al. A master attack methodology for an AI-based automated attack planner for smart cities. IEEE;6:48360–73.

70 Angelini M, Santucci G. Visual cyber situational awareness for critical infrastructures. In: 8th ISVICI. 2015. p. 83–92.

71 Wang P, Ali A, Kelly W. Data security and threat modeling for smart city infrastructure. In: 2015 international conference on cyber security of smart cities, industrial control system and communications (SSIC), 2015. p. 1–6.

72 Wang SP, Ledley RS. Computer architecture and security: fundamentals of designing secure computer systems. New York: Wiley; 2012.

73 Bou-Harb E, Neshenko N. Cyber threat intelligence for the internet of things. New York: Springer; 2020.

74 Naik DR, Das LB, Bindiya TS. Wireless sensor networks with Zigbee and WiFi for environment monitoring, traffic management and vehicle monitoring in smart cities. In: 2018 IEEE 3rd international conference on computing, communication and security (ICCCS). 2018. p. 46–50.

75 Dowling S, Schukat M, Melvin H. A ZigBee honeypot to assess IoT cyberattack behavior. In: 2017 28th ISSC. 2017. p. 1–6.

76 Oza P, Foruhandeh M, Gerdes R, Chantem T. Secure traffic lights: replay attack detection for model-based smart traffic controllers. In: Proceedings of the second ACM workshop on automotive and aerial vehicle security. 2020. p. 5–10.

77 He Y, Mendis GJ, Wei J. Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans Smart Grid. 2017;8(5):2505–16. https ://doi.org/10.1109/TSG.2017.27038 42.

78 Azmoodeh A, Dehghantanha A, Choo K-KR. Robust malware detection for internet of (battlefield) things devices using deep Eigenspace learning. IEEE Trans Sustain Comput. 2018;4(1):88–95.

79 Dovom EM, Azmoodeh A, et al. Fuzzy pattern tree for edge malware detection and categorization in IoT. J Syst Archit. 2019;97:1–7.

80 Kumar A, Lim TJ. EDIMA: early detection of IoT malware network activity using machine learning techniques. In: 2019 IEEE 5th world forum on internet of things (WF-IoT). 2019. p. 289–94. https ://doi.org/10.1109/WFIoT.2019.87671 94.

81 Meidan Y, et al. N-baiot—network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Comput. 2018;17(3):12–22.

82 Alazab VRM, et al A visualized botnet detection system based deep learning for the internet of things networks of smart cities. IEEE Trans Ind Appl. 2020.

83 Raza S, Wallgren L, Voigt T. SVELTE: real-time intrusion detection in the internet of things. Ad Hoc Netw. 2013;11(8):2661–74.

84 Shreenivas D, Raza S, Voigt T. Intrusion detection in the RPL-connected 6LoWPAN networks. In: Proceedings of the 3rd ACM international workshop on IoT privacy, trust, and security. 2017. p. 31–8.

85 Li D, Chen D, Goh J, Ng S. Anomaly detection with generative adversarial networks for multivariate time series. ArXiv Prepr. ArXiv180904758. 2018.

86 Azmoodeh A, et al. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. J Ambient Intell Humaniz Comput. 2018;9(4):1141–52.

87 Baracaldo N, Chen B, Ludwig H, Safavi A, Zhang R. Detecting poisoning attacks on machine learning in IoT environments. In: 2018 IEEE international congress on internet of things (ICIOT). 2018. p. 57–64.

88 Laishram R, Phoha VV. Curie: a method for protecting SVM classifier from poisoning attack. ArXiv Prepr. ArXiv160601584. 2016.

89 Goodfellow I, et al. Deep learning. Cambridge: MIT Press; 2016.

90 Hinton GE. Deep belief nets. 2010.

91 Senge R, Hüllermeier E. Fast fuzzy pattern tree learning for classification. IEEE Trans Fuzzy Syst. 2015;23(6):2024–33.

92 Goodfellow I, et al. Generative adversarial nets. In: Advances in neural information processing systems. Cambridge: MIT Press; 2014. p. 2672–80.

93 Edelkamp S, Schrödl S. Chapter 1—Introduction. In: Edelkamp S, Schrödl S, editors. Heuristic search. San Francisco: Morgan Kaufmann; 2012. p. 3–46.

94 Sanders WH, Meyer JF. Stochastic activity networks: formal definitions and concepts. In: School organized by the European Educational Forum. 2000. p. 315–43.

95 Chiola G, Dutheillet C, Franceschinis G, Haddad S. Stochastic well-formed colored nets and symmetric modeling applications. IEEE Trans Comput. 1993;42(11):1343–60.

96 David HA, Moeschberger ML. The theory of competing risks. London: Charles Griffin and Company; 1978.

97 Dondossola G, Garrone G, Szanto J, Deconinck G, Loix T, Beitollahi H. ICT resilience of power control systems:

98 experimental results from the CRUTIAL testbeds. In: 2009 IEEE/IFIP international conference on dependable systems & networks. 2009. p. 554–9.

99 Goh J, et al. A dataset to support research in the design of secure water treatment systems. In: ICCIIS. 2016. p. 88–99.

100 Shodan. Доступно: http://shoda n.io. Дата доступу: 21.11.23.

101 UCSD network telescope—near-real-time network telescope dataset. www.caida.org. Дата доступу: 21.11.23.

102 Rinaldi SM, et al. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst Mag. 2001;21(6):11–25.

103 Shameli-Sendi A, Aghababaei-Barzegar R, Cheriet M. Taxonomy of information security risk assessment (ISRA). Comput Secur. 2016;57:14–30.

104 Aven T, Heide B. Reliability and validity of risk analysis. Reliab Eng Syst Saf. 2009;94(11):1862–8.

105 Nurse JRC, Creese S, Roure DD. Security risk assessment in internet of things systems. IT Prof. 2017;19(5):20–6.

106 Xin Y, et al. Machine learning and deep learning methods for cybersecurity. IEEE;6:35365–81. 106. Thomas JJ, Cook KA. A visual analytics agenda. IEEE Comput Graph Appl. 2006;26(1):10–3.

107 Lecun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, vol. 521, no. 7553, pp. 436–444, 2015.

108 M. Amine, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection : Approaches , datasets , and comparative study,” J. Inf. Secur. Appl., vol. 50, p. 102419, 2020.

109 N. Hasan, R. N. Toma, et al, “Electricity Theft Detection in Smart Grid Systems : A CNN-LSTM Based Approach,” Electr. Th. Detect. Smart Grid Syst. A CNN-LSTM Based Approach, vol. 12, no. 17, p. 3310, 2019.

110 D. Kwon, et al, “An Empirical Study on Network Anomaly Detection using Convolutional Neural Networks,” in In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018, pp. 1595–1598.

111 H. Liu, B. Lang, M. Liu, and H. Yan, “Knowledge-Based Systems CNN and RNN based payload classification methods for attack detection,” Knowledge-Based Syst., vol. 163, pp. 332–341, 2019.

112 F. Bolelli, L. Baraldi, F. Pollastri, and C. Grana, “A Hierarchical QuasiRecurrent approach to Video Captioning,” IEEE IPAS, 2018, pp. 162–167.

113 S. Merity, C. Xiong, and R. Socher, “Quasi-Recurrent Neural Network,” in arXiv, 2017, pp. 1–11.

114 M. Wang et al., “Quasi-fully Convolutional Neural Network with Variational Inference for Speech Synthesis,” in ICASSP 2019-2019 IEEE ICASSP, 2019, pp. 7060–7064.

115 J. Huang and Y. Feng, “Optimization of Recurrent Neural Networks on Natural Language Processing,” in Proceedings of the 2019 8th International Conference on Computing and Pattern Recognition, 2019, pp. 39–45.

116 P. Wu, H. Guo, and N. Moustafa, “Pelican : A Deep Residual Network for Network Intrusion Detection,” arXiv, vol. 2001.08523, 2020.

117 D. Yao, et al, “Energy Theft Detection With Energy Privacy Preservation in the Smart Grid,” IEEE Internet Things J., vol. 6, no. 5, pp. 7659–7669, 2019.

118 Financial news of Ukraine (2018), “IT of Ukraine. Help can not be disturbed”. Доступно: https://news.finance.ua/ Дата доступу: 20.11.23.

119 Hi-Tech Business News (2018), “Trends in IT outsourcing in Ukraine”, Доступно: http://startupline.com.ua/ Дата доступу: 20.11.23.

120 Riskxchange (2022) «10 Effective IT Security Risk Assessment Tactics», Доступно: https://riskxchange.co/Дата доступу: 20.11.23.

121 ПНУ ім. Стефаника. Кафедра хімії. «Державна система моніторингу довкілля» Доступно: kc.pnu.edu.ua, Дата доступу: 20.11.23.

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

123Najla, A. T., Abbas, S. N., & Sujata, D. (2020). Cyber threat intelligence for secure smart city. arXiv preprint arXiv:2007.13233.

ДОДАТКИ

Додаток А

Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XI НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

13-14 грудня 2023 року

ТЕРНОПІЛЬ
2023

УДК 004.732
Базан І.В., Коваль А.А.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИЯВЛЕННЯ КІБЕРАТАК В «РОЗУМНОМУ МІСТІ» НА ОСНОВІ МАШИННОГО НАВЧАННЯ

I. Bazan, A. Koval

DETECTING CYBERATTACKS IN A SMART CITY BASED ON MACHINE LEARNING

Технологічні винаходи змінили динаміку розвитку світу. Інфраструктура в кожній галузі автоматизується за допомогою Інтернету речей та бездротових мереж зв'язку. «Розумні міста» формуються на бездротовому зв'язку, де інфраструктура за своєю природою уможливлює велику кількість кібератак. Тому вразливості в «розумних містах» потребують належного вирішення. Сфера «розумних міст» досить різноманітна і має багато застосувань, включаючи електронний уряд, «розумні» будинки, інтелектуальний транспорт, телемедицину, «розумні» мережі, моніторинг, енергетику та багато іншого [1].

Безпека мереж передачі даних є темою для багатьох дослідників у всьому світі через постійне зростання кількості кібератак. Система виявлення вторгнень - це система, яка повинна ідентифікувати фальшиві пакети даних. Оптимальний алгоритм системи виявлення вторгнень балансує між високою точністю та показниками хибнонегативних і хибнопозитивних спрацьовувань. Крім того, основною її метою є виявлення можливих кібератак. «Розумні міста» потребують захищених каналів зв'язку, тому система виявлення вторгнень відіграє важливу роль [2]. Різноманітні технології, такі як ланцюги Маркова, машинне навчання, оптимізація та пуассонівський розподіл, використовуються для покращення систем виявлення сигнатур, аномалій та гібридних вторгнень.

Мережі IoT є вразливими до кібератак, тому в «розумному місті» протидія таким загрозам є великим викликом. DOS, DDOS, Sybil-атаки, SQL-ін'єкції та атаки зловмисного програмного забезпечення є поширеними типами атак в середовищі IoT, тому «розумні міста» постійно піддаються цим атакам. Результатом незахищеної мережі сенсорних вузлів може бути збій системи або припинення роботи сервісу, якщо не застосовувати превентивні засоби для забезпечення надійності і захищеності.

Існує багато рішень, які можуть бути використані відповідно до потреб захисту [3]. Найкращим підходом у виявленні різних загроз у «розумних містах» є машинне навчання. Машинне навчання для виявлення кіберзагроз у мережах «розумного міста». Існує три основні типи підходів машинного навчання: на основі аномалій, на основі сигнатур та гібридний. Виявлення на основі аномалій відбувається за допомогою інтелекту системи, навченого різними методами, підхід на основі сигнатур порівнює мережевий трафік з існуючими сигнатурами або шаблонами атак, що призводить до виявлення загроз, а гібридна система є сумішшю активів обох підходів, що робить її більш ефективною та точною, ніж обидва. Залежно від сценаріїв середовища, різні дослідники розробили різні типи системи виявлення вторгнень, використовуючи різні підходи, алгоритми з різними цільовими системами і порівнюючи точність і достовірність запропонованого ними алгоритму з іншими алгоритмами в своїх тематичних дослідженнях .

Література

1. Cimen, H., Palacios-García, E. J., et al. Smart-Building Applications: Deep Learning-Based, Real-Time Load Monitoring. IEEE Industrial Electronics Magazine, 15(2), 4-15.

2. Rincy N, T., & Gupta, R. Design and development of an efficient network intrusion detection system using machine learning techniques. Wireless Communications and Mobile Computing, 2021, 1-35.

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

УДК 004.73:681.55
Коваль А.А., Базан І.В.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

КІБЕРФІЗИЧНІ СИСТЕМИ: ВИКЛИКИ В СКЛАДНИХ МЕРЕЖАХ І РОЗПОДІЛЕНИХ СИСТЕМАХ

A. Koval, I. Bazan

CYBER-PHYSICAL SYSTEMS: CHALLENGES IN COMPLEX NETWORKS AND DISTRIBUTED SYSTEMS

Складні мережі є невід'ємною частиною повсякденного життя. Прикладами таких мереж є транспортні та телефонні мережі, інтернет, тощо. В останнє десятиліття аналіз і керування складними мережами, що складаються з декількох динамічних вузлів, привертає велику увагу в різних галузях. Зокрема, було закладено основи керування та синхронізації великих складних динамічних мереж з певними типами топології. У математиці складну динамічну мережу можна описати за допомогою графа. Кожен вузол такого графа представляє фундаментальний елемент з певною динамікою, а межі представляють інтерактивну топологію мережі. Розробка систем розпізнавання топології є важливим аспектом в складних мережах. Застосування таких систем можна знайти в різних галузях науки і техніки. Наприклад, якщо в мережі зв'язку, електромережі або Інтернеті трапляється значна несправність, дуже важливо визначити місце розташування дефектної ділянки, що стає можливим із застосуванням систем розпізнавання топології.

Задумані і реалізовані мережеві системи управління стикаються з багатьма проблемами, пов'язаними з обчислювальним часом, програмним забезпеченням, змінними часовими затримками, відмовами, реконфігурацією і розподіленими системами підтримки прийняття рішень. Розробка протоколу, що гарантує якість обслуговування в реальному часі в бездротових мережах, узгодження між дизайном закону управління і складністю реалізації в реальному часі, подолання різниці між системами безперервного і дискретного часу, а також надійність великомасштабних систем – виклики, які стоять в галузі кіберфізичних систем (КФС). Високі вимоги до надійності та безпеки гетерогенних компонентів, які взаємодіють у складному, комбінованому фізичному середовищі і працюють у кількох просторових і часових масштабах, вимагають застосування фреймворків, алгоритмів, методів і ресурсів. Математична модель, фізична модель, аналіз і алгоритм, дизайн системи і розподіл, з пов'язаними з ними непередбачуваністю і ризиком, є фундаментальними теоріями фізичного світу. Ключовим елементом КФС є давачі які є апаратними мостами між фізичним і кібернетичним світом, для яких необхідні методи обробки сигналів. У комплексному погляді КФС включає в себе стабільність, оптимізацію і управління розподіленими і цифровими системами.

Розподілені кіберфізичні алгоритми, які можуть бути використані в CPS для виявлення та аналізу подій, надають кожному вузлу повну інформацію системи навіть при зміні топології. CPS охоплюватиме різні аспекти соціального та економічного життя, матиме широкий вплив і стане орієнтиром для комп'ютерних наук та інших галузей. Очікується, що при проектуванні та виробництві майбутніх інженерних систем з новими технологіями, які значно перевищують сучасні стандарти автономності, функціональності, доступності, надійності та захисту даних, кіберфізичні системи матимуть важливе значення.

Література

1. Xia, Y., et al (2019). Introduction to focus issue: Complex network approaches to cyber-physical systems. Chaos: An Interdisciplinary Journal of Nonlinear Science, 29(9).

2. Mishra, A., et al (2023). Emerging technologies and design aspects of next generation CPS with a smart city application perspective. IJSAEM, 14(Suppl 3), 699-721.

3. Canizo, M., Conde, A., Charramendieta, S., Minon, R., Cid-Fuentes, R. G., & Onieva, E. (2019). Implementation of a large-scale platform for cyber-physical system real-time monitoring. IEEE Access, 7, 52455-52466.